НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»
УДК 004.056

«До захисту допущено»
В.о. завідувача кафедри
_____ М.В.Грайворонський
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Метод оцінювання ефективності контролів безпеки

Виконав (-ла): студент (-ка) 2 курсу, групи ФБ-71мп
(шифр групи)

Соловйов Данило Русланович
(прізвище, ім’я, по батькові)

Науковий керівник к.т.н., доц. Барановський Олексій Миколайович_ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н., ст. викл. ОНАЗ Височіненко М.С. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою
Спеціальність (спеціалізація) – 125 Кібербезпека («Системи і технології кібербезпеки)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)

«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Соловйову Данилу Руслановичу

1. Тема дисертації: Метод оцінювання ефективності контролів безпеки

науковий керівник дисертації к.т.н., доц. Барановський Олексій Миколайович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «15» листопада 2018 р. № 4171-с

2. Термін подання студентом дисертації 12.12.2018 р.

3. Об'єкт дослідження _____
_____

4. Вихідні дані _____
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____
_____
_____

7. Орієнтовний перелік публікацій _____
_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ (підпис) _____ (ініціали, прізвище)

Науковий керівник дисертації _____ (підпис) _____ (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Робота складається з 94 сторінок, і містить 4 ілюстрацій, 39 таблиці та 15 джерел.

Метою даної роботи є дослідження підходів до оцінювання ефективності контролів безпеки та реалізація методу оцінювання ефективності контролів безпеки. Для досягнення поставленої мети у роботі було проведено аналіз підходів до оцінювання ефективності контролів безпеки. За результатами аналізу було обрано для подальшої роботи два підходи для оцінки ефективності, а саме матричний та експертна оцінка. Запропоновано метод оцінювання ефективності контролів безпеки створений на їх основі та описано основні етапи реалізації даного методу.

Експериментальним шляхом на основі пасивних контролів безпеки досліджена практична реалізація методу, проаналізовані практичні результати експерименту та зроблено висновок, щодо ефективності тестових контролів та працездатності самого методу.

Результатом роботи є метод, що дозволяє оцінювати ефективність контролів безпеки, та є працездатним.

Ключові слова: ЕФЕКТИВНІСТЬ, КОНТРОЛЬ, SIEM, РИЗИКИ, ЕКСПЕРТНА ОЦІНКА, МАТРИЧНИЙ МЕТОД.

ABSTRACT

The work consists of 94 pages and contains 4 illustrations, 39 tables and 15 sources.

The purpose of this work is to study the approaches to assessing the effectiveness of security controls and implement a method for assessing the effectiveness of security controls. To achieve this goal, an analysis of approaches to assessing the effectiveness of security controls was conducted. Based on the results of the analysis, two approaches for assessing efficiency were chosen for further work, namely matrix and expert evaluation. The method of assessing the effectiveness of safety controls created on their basis is proposed and the main stages of the implementation of this method are described.

Experimental test on the basis of passive security controls was the practical realization of the method, the practical results of the experiment were analyzed and a conclusion was made regarding the effectiveness of the test controls and the performance of the method itself.

The result of the work is a method that allows assessing the effectiveness of security controls, and is operational.

Key words: EFFICIENCY, CONTROL, SIEM, RISKS, EXPERT ASSESSMENT, MATRIX METHOD.

РЕФЕРАТ

Работа состоит из 94 страниц и содержит 4 иллюстраций, 39 таблицы и 15 источников.

Целью данной работы является исследование подходов к оценке эффективности контролей безопасности и реализация метода оценки эффективности контролей безопасности. Для достижения поставленной цели в работе был проведен анализ подходов к оценке эффективности контролей безопасности. По результатам анализа был выбран для дальнейшей работы два подхода для оценки эффективности, а именно матричный и экспертная оценка. Предложен метод оценки эффективности контролей безопасности созданный на их основе и описаны основные этапы реализации данного метода.

Экспериментальным путем на основе пассивных контролей безопасности исследована практическая реализация метода, проанализированы практические результаты эксперимента и сделан вывод относительно эффективности тестовых контролей и работоспособности самого метода.

Результатом работы является метод, что позволяет оценивать эффективность контролей безопасности и является работоспособным.

Ключевые слова: ЭФФЕКТИВНОСТЬ, КОНТРОЛЬ, SIEM, РИСКИ, ЭКСПЕРТНЫЕ ОЦЕНКИ, МАТРИЧНЫЙ МЕТОД.

ЗМІСТ

ПЕРЕЛІК ВИКОРИСТАНИХ СКОРОЧЕНЬ, ТЕРМІНІВ, ОДИНИЦЬ, ПОЗНАЧЕНЬ

АС	автоматизована система
ІБ	інформаційна безпека
ІПКС	інцидент/потенційна кризова ситуація
ІР	інформаційні ресурси
ІС	інформаційна система
СЗІ	система захисту інформації

ВСТУП

Актуальність дослідження. Інформаційні системи значно поліпшили продуктивність підприємств. Проте, повна залежність інформаційних систем від критичних операцій зробила підприємства схильними до атак з мережі. Оскільки залежність економіки від інформаційних систем зростає, фінансові втрати від порушення інформаційної безпеки також збільшуються. Цей ризик фінансових втрат у зв'язку з порушенням інформаційної безпеки є причиною для занепокоєння і корпорації, і уряду. У більшості організацій не існує повної картини стану своєї інформаційної безпеки та ризиків. Як правило, спеціальні рішення щодо безпеки засновані на реалізації керівних принципів і документів, виданих державними установами або сторонніми організаціями. Інформаційні відділи можуть підтримувати існуючий рівень безпеки в перевірці, але підприємству дуже складно мати чітку картину стану своєї інформаційної безпеки без формального аналізу ризиків. Персонал інформаційних відділів може бути компетентним в методах реалізації засобів безпеки, але йому часто не вистачає досвіду в фінансовому моделюванні та аналізі ризиків.

Методологія формального аналізу ризиків добре вивчена в деяких областях науки (фінанси, інженерія, авіація та ін..). Однією з проблем, пов'язаною з аналізом ризиків інформаційної безпеки, є відсутність стандартизованих показників і методів для оцінки виміру впливу загроз і оцінки в інтересах контролю і гострої нестачі статистичних даних для оцінки ризиків. Ще однією проблемою є низька якість даних щодо факторів ризику і слабкі місця. Це викликано тим, що організації побоюються розголошення інцидентів порушення інформаційної безпеки, тому що це може залучити нових хакерів. Нарешті, процес аналізу інформаційних ризиків дуже слабо висвітлений у керівних документах, є дорогим і вимагає глибокого вивчення внутрішньої структури організації. Тому більшість організацій найчастіше обмежується зовнішньою оцінкою ризиків і проводять такі оцінки періодично (щорічно або два рази на рік), а не безперервно. Крім того, у організації

немає можливості визначити якість зробленої оцінки, і вони змушені покладатися на висновки, зроблені сторонніми консультантами.

Мета та завдання дослідження. Метою даної роботи є дослідження підходів до оцінювання ефективності контролів безпеки та реалізація методу оцінювання ефективності контролів безпеки. Для досягнення поставленої мети у роботі необхідно виконати низку завдань:

- визначити механізми оцінювання ефективності контролів безпеки;
- провести аналіз підходів до оцінювання ефективності контролів безпеки;
- описати метод оцінювання ефективності контролів безпеки;
- навести структуру системи оцінювання ефективності контролів безпеки;
- побудувати систему оцінювання ефективності контролів безпеки;
- дослідити практичну реалізацію методу оцінювання ефективності контролів безпеки.

Об'єкт та предмет дослідження. Об'єктом даної роботи є механізми контролю безпеки. Предметом виступають методи та процеси розробки системи оцінювання ефективності контролів безпеки.

Методи дослідження. У рамках даного дослідження були використані наступні методи: вивчення та аналіз наукової літератури; системний і порівняльний аналіз; дедукція – вид умовиводу від загального до окремого, від абстрактного до конкретного; моделювання; конструювання та проектування.

Наукова новизна дослідження. Наукова новизна дослідження полягає в тому, що:

запропоновано оригінальний алгоритм оцінювання ефективності контролів безпеки. Як наслідок, алгоритм виключає можливість здійснення автоматичного і автоматизованого аналізу контролів безпеки; забезпечує захист від атак, дешифрування;

реалізована система інтелектуального-адаптивного оцінювання ефективності контролів безпеки, що забезпечує ефективне функціонування в умовах атак.

Практична значущість роботи полягає в тому, що результат досягнення поставленої мети має можливість застосування в діяльності конкретної установи, а також може бути використаний і іншими установами для вдосконалення системи оцінювання ефективності контролів безпеки на підприємстві, також дана концепція викладу даного дослідження може бути використана в якості методичного посібника при розробці системи оцінювання ефективності контролів безпеки.

Структура роботи включає в себе перелік умовних скорочень, вступ, чотири розділи, висновок, список літератури. Загальний обсяг роботи 94 сторінок.

1 ТЕОРЕТИЧНИЙ АСПЕКТ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОНТРОЛІВ БЕЗПЕКИ

В даному розділі будуть розглянуті основні етапи обробки інцидентів, зазначені методи підрахунку та обробки експертних оцінок та визначені основні поняття, що стосуються ефективності контролів ІБ.

1.1 Інформаційна безпека підприємства: сутність, принципи, нормативна складова та процедура управління інцидентами безпеки

У наш час швидкість створення новітніх засобів захисту майже не відрізняється від швидкості появи методів та механізмів їх зламу. Зловмисники завжди прагнуть знайти можливість створити засоби для реалізації загроз. Безпека інформаційного середовища сучасного підприємства є важливою складовою у будь-якому бізнес-процесі, та вже важко уявити підприємство без захищеної інформаційної системи. Тому що інформація стала найбільш цінним ресурсом і її втрата може привести до значних втрат.

Проте, не зважаючи на вже запропоновані захисні системи все одно залишається багато не вирішених проблем. Отже, для того щоб покращити захист інформаційного середовища та знизити кількість інцидентів необхідно звернутися до досвіду управління інцидентами, що використовується в усьому світі.

Згідно ISO/IEC 27035-1:2016[1] інцидент інформаційної безпеки (information security incident): одна або серія небажаних або несподіваних подій інформаційної безпеки, які мають значну ймовірність компрометації бізнес-операції і загрожують інформаційній безпеці. Модель інциденту інформаційної безпеки наведена на рисунку 1.1.

Рисунок 1.1 – Модель інциденту інформаційної безпеки

Міжнародний стандарт ISO 27001:2013[2] звертає особливу увагу на необхідність створення процедури управління інцидентами інформаційної безпеки – очевидно, що без своєчасної реакції на інциденти безпеки та усунення їх наслідків неможливе ефективне функціонування системи управління інформаційною безпекою. На жаль, в процесі аудиту різних інформаційних систем доводиться стикатися з безліччю проблем реєстрації та розслідування інцидентів, які свідчать про те, що стандартам на підприємствах приділяється дуже мало уваги. [3]

Основною метою процесу управління інцидентами (Incident Management) є відновлення працездатності систем як можна швидше і мінімізація несприятливих наслідків на роботу підприємства, що забезпечить узгоджений рівень якості послуги.

Організація процесу реагування на інцидент переслідує наступні цілі:

- підтвердити або спростувати факт інциденту;
- попередити не скоординовані дії служб при усуненні наслідків інциденту;
- при виникненні інциденту відновити працездатність компанії в найкоротші терміни;
- представити детальний звіт про інцидент, що стався;
- представити корисні рекомендації щодо недопущення подібних інцидентів у майбутньому;

– створити умови для накопичення в базі даних точної інформації про інциденти та шляхи усунення наслідків;

– забезпечити якнайшвидше виявлення (попередження) інцидентів у подальшому шляхом удосконалення політики ІБ, модернізації системи ІБ);

– забезпечити цілісність доказів інциденту;

– створити умови для порушення кримінальної справи проти зловмисників;

– мінімізувати наслідки інциденту;

– захистити репутацію компанії;

– провести навчання співробітників компанії процесу реагування на інцидент.[4]

На сьогоднішній день розроблено достатню кількість організаційних документів, у яких описані питання управління інцидентами ІБ.

Так, подібні питання описані в:

1) ISO/IEC 27001:2013 Information security management system. Вимога. В даному документі висуваються загальні вимоги до побудови системи управління інформаційної безпеки, які стосуються в тому числі і процесів управління інцидентами.

2) ISO/IEC 27035-1:2016 Information security incident management. Даний документ описує інфраструктуру управління інцидентами в межах циклічної моделі PDCA. Даються докладні специфікації для стадій планування, експлуатації, аналізу і поліпшення процесу. Розглядаються питання забезпечення нормативно-розпорядчою документацією, ресурсами, даються докладні рекомендації щодо необхідних процедур.

3) CMU/SEI-2004-TR-015 Defining incident management processes for CISRT. Цей документ описує методологію планування, впровадження, оцінки і поліпшення процесів управління інцидентами. Основний упор робиться на організацію роботи CISRT (Critical Incident Stress Response Team) — групи або підрозділу, що забезпечує сервіс і підтримку запобігання, обробки і реагування на інциденти інформаційної безпеки. Вводиться ряд критеріїв, на підставі яких можна оцінювати ефективність даних сервісів, наводяться докладні процесні карти.

4) NIST SP 800-61 Computer security incident handling guide. Тут представлений збірник "кращих практик" з побудови процесів управління інцидентами та реагування на них. Докладно розбираються питання реагування на різні типи загроз, такі як поширення шкідливого програмного забезпечення, несанкціонований доступ та інші.

Окрім названих методологій з управління інцидентами існує значна кількість інших. Питання вибору підходу цілком залежить від організації та особливості функціонування бізнес процесів. Проте варто слідкувати за тим, щоб обрана методологія відповідала сучасними стандартами систем управління.

Відсутність процедури управління інцидентами – є звичайною проблемою у багатьох компаніях. Але відсутність інцидентів не свідчить про система є безпечною, а означає лише, що інциденти не фіксуються або не визначаються. Підприємства мають наступні складнощі підчас роботи з інцидентами.

Визначення інциденту. У компанії відсутня методика визначення інцидентів, а співробітники не знають, які події є інцидентами. Це особливо важливо у випадку інцидентів інформаційної безпеки – вони не завжди заважають нормальній роботі. Наприклад, інцидентом безпеки буде залишення без нагляду на столі конфіденційних документів, на що ніхто не може і не звернути уваги, а зловмисник (який може бути співробітником компанії) такі документи помітить.

Оповіщення про виникнення інциденту. Співробітники компанії часто не інформовані про те, кого і в якій формі слід ставити в популярність при виникненні інциденту, – наприклад, не визначено ні форми звітів, ні перелік осіб, яким необхідно надсилати звіти про інциденти. Навіть якщо співробітник помітить, що його колега уносить для роботи додому конфіденційні документи компанії, він не завжди знає, які дії слід робити в даній ситуації.

Реєстрація інциденту. Відповідальним особам (навіть якщо вони призначені) часто не надається методика реєстрації інцидентів – не існує спеціальних журналів їх реєстрації, а також правил і термінів заповнення.

Усунення наслідків і причин інциденту. У компаніях, як правило, відсутня документально зафіксована процедура описує дії, які необхідно виконати з метою

усунення наслідків і причин інциденту. У першу чергу, така процедура повинна передбачати, щоб заходи по усуненню наслідків і причин інциденту не порушували процедури їх розслідування: усунення наслідків інциденту не має «замітати сліди», щоб неможливо було встановити винних в інциденті.

Розслідування інциденту. На етапі розслідування інцидентів основну роль відіграють: ведення журналів реєстрації подій, чітке розділення повноважень користувачів, відповідальність за виконані дії – важливі докази того, хто брав участь у інциденті і які дії він виконував. На жаль, про розслідування інцидентів в компаніях часто просто забувають. Як тільки наслідки інциденту усунені і бізнес-процеси відновлені, подальші дії з розслідування інциденту і здійснення коригувальних і превентивних заходів не виконуються.

Реалізація дій, що попереджають повторне виникнення інциденту. Як правило, якщо компанії було завдано якоїсь шкоди, то до винних у виникненні інциденту (які визначені без необхідних у таких випадках процедур) все ж застосовуються різні стягнення, однак внесення дисциплінарних стягнень не завжди підпорядковується затвердженим процедурам та інші дії по запобіганню повторення інциденту виконуються теж не завжди. [3]

Впровадження процедури управління інцидентами – важливий крок в управлінні інформаційною безпекою. Важливо правильно і своєчасно усунути наслідки інциденту. Необхідно розслідувати інцидент, що включає визначення причин його виникнення та винних осіб. Варто виконати оцінку необхідності дій щодо усунення причин інциденту, якщо потрібно – реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту. Крім цього, важливо зберігати всі дані про інциденти інформаційної безпеки, так як статистика інцидентів інформаційної безпеки допомагає усвідомлювати їх кількість і характер, а також зміну в часі. За допомогою інформації про статистику інцидентів можна визначити найбільш актуальні загрози для компанії і, відповідно, максимально точно планувати заходи по підвищенню рівня захищеності інформаційної системи компанії.

Важливим етапом в створенні процедури управління інцидентами безпеки є визначення переліку подій, які будуть класифікуватися як інцидент. Адже події, що не визначені у процедурі будуть вважатися нормальними для системи навіть, якщо вони несуть шкоду.

Для опису процедури управління інцидентами безпеки використовується класична модель безперервного поліпшення процесів, що отримала назву від циклу Шухарта-Демінга – модель PDCA (Плануй, Plan – Виконуй, Do – Перевіряй, Check – Дій, Act). [5]

Стандарт ISO 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Природно, що і процедура управління інцидентами підпорядковується моделі PDCA.

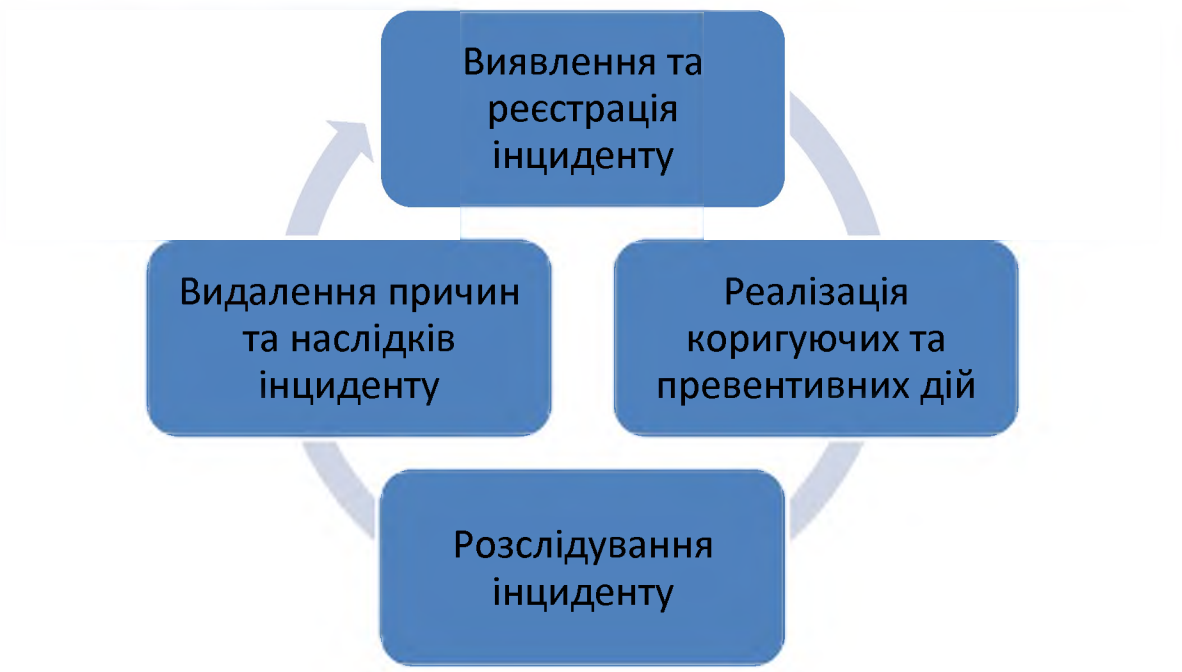

Рисунок 1.2 – Модель PDCA

Виявлення та реєстрація інциденту

Виявлення інциденту інформаційної безпеки може бути проведене будь-яким співробітником. Тому варто впровадити інструкцію, що зазначає, як користувач має повідомити про появу інциденту та перелік дій, що потрібно виконати

користувачу після виявлення інциденту. Після впровадження даної інструкції, першочергова обробка інцидентів буде проводитися більш організовано та ймовірність не виявлення інциденту, через відсутність дій користувача значно зменшиться.

Також необхідно впровадити відповідну інструкцію для особи, відповідного за реєстрацію інцидентів, що буде містити правила і термін реєстрації інциденту, перелік необхідних інструкцій для працівника, що виявив інцидент, порядок контролю за усуненням наслідків і причин інциденту.

Усунення причин, наслідків інциденту і його розслідування

Інструкція по усуненню причин і наслідків інциденту включає опис загальних дій, які необхідно зробити (конкретні дії для кожного виду інциденту визначати трудомістко і не завжди доцільно), а також терміни, протягом яких слід усунути наслідки та причини інциденту. Терміни усунення наслідків і причин інциденту залежать від рівня інциденту. Слід розробити класифікацію інцидентів – визначити кількість рівнів критичності інцидентів, описати інциденти кожного рівня і терміни їх усунення.

Таким чином, інструкція по усуненню наслідків і причин інциденту може включати: опис дій, що вживаються для усунення наслідків і причин інциденту, терміни усунення і вказівка на відповідальність за недотримання інструкції.

Розслідування інциденту включає в себе визначення винних у його виникненні, збір доказів інциденту, визначення відповідних дисциплінарних стягнень. Інструкція з розслідування описує: дії з розслідування інциденту (в тому числі визначення винних у його виникненні), правила збору та зберігання доказів (особливо у разі, якщо може знадобитися використання доказів у судових органах) і правила внесення дисциплінарних стягнень.

Реалізація коригуючих та превентивних дій

Після усунення наслідків інциденту і відновлення нормального функціонування бізнес-процесів компанії, можливо, буде потрібно виконати дії щодо запобігання повторного виникнення інциденту. Для визначення необхідності реалізації таких дій слід провести аналіз доцільності коригувальних і превентивних

дій. В деяких випадках наслідки інциденту незначні порівняно з коригуючими і превентивними діями, і тоді доцільно не робити подальших кроків після усунення наслідків інциденту.

Ключовою вимогою до функціонування даної процедури управління інцидентами інформаційної безпеки є послідовне та безперервне повторення описаних етапів моделі PDCA, для аналізу інцидентів в системі та подальшого перегляду визначених як інциденти ситуацій.

В управлінні інцидентами інформаційної безпеки важливо, перехоплювати всі інциденти, проводити детальне розслідування, визначати винних та впроваджувати запобіжні дії, для подальшого уникнення повторної появи інциденту. Інциденти у сфері ІБ не завжди можливо перехопити або легко відслідкувати, проте збитки після інцидентів після реалізації загроз зазвичай дуже значні. Тому наявність гарно відпрацьованої процедури управління інцидентами ІБ у наш час є необхідністю.

Проте варто усвідомлювати, що впроваджена процедура управління не забезпечить превентивний захист та не збереже компанію від збитків. Але воно дозволяє знизити ймовірність повторення інциденту після внесених коригувальних дій та ймовірність вдалої реалізації загрози. Статистичні показники інцидентів інформаційної безпеки представляє особливу цінність для компанії як показники ефективності функціонування системи управління інформаційною безпекою.

На сьогоднішній день, перевірка ефективності введених контролів інцидентів інформаційної безпеки стоїть досить гострим питанням та вимагає значних коштів для проведення.

Методами оцінки ефективності тих чи інших механізмів захисту в даний час є наступні:

•організація збору та статистична обробка даних з питань інформаційної безпеки на реально функціонуючих системах;

• постановка натурних експериментів;

• статистичне або імітаційне моделювання;

• експертні оцінки.

Визнаючи важливість і необхідність використання перших трьох із зазначених методів, в даний час основну увагу приділимо методу експертних оцінок, відповідно до якого і можуть бути отримані характеристики певних механізмів захисту в умовах тих чи інших впливів порушника.

Метод експертних оцінок пов'язаний з об'єднанням знань найбільш компетентних осіб в області досліджуваних програм. Для реалізації методу експертних оцінок створюється група експертів (в зарубіжних джерелах її називають дельфійською групою), що здійснює збір інформації з різноманітних джерел з визначеної проблеми. Її члени повинні володіти найвищим рівнем обізнаності про стан справ по аналізованій проблемі. Головна перевага даного методу оцінки то, що аналіз ризику може бути виконаний в короткий час. Природно, витрати часу залежать від складності та обсягу розв'язування задачі.

При створенні системи забезпечення ІБ для обговорення різних загроз ІБ і вразливих місць, що лежить в основі критеріїв прийняття рішень, повинна бути створена дельфійська група, яка перш за все повинна ідентифікувати загрози ІБ за ступенем ризику і виробити рішення про те, які види загроз вони вважають найнебезпечнішими. З огляду на експертні знання і думки кожного, група може прийти до безлічі узгоджених висновків, сформульованих у вигляді упорядкованого, наприклад, у напрямку убування небезпеки загроз ІБ, списку.

Критерій оцінки, що використовується дельфійською групою, може будуватися за принципом найбільшого ризику, ступеня секретності, важливості, вартості, небезпеки, витрат часу, наслідків фінансових збитків, ймовірності виникнення загрози і ін.

Оцінка ефективності забезпечення ІБ пов'язана з оцінкою ризику ІБ. Експерт може з'ясувати, які з засобів забезпечення ІБ (наприклад, апаратне або програмне забезпечення) передбачається використовувати, а потім, використовуючи, наприклад, методологію якісного аналізу, застосувати відповідні критерії оцінки для того, щоб визначити, чи є даний механізм захисту сильним або слабким в порівнянні з іншими реалізаціями цих же коштів з присвоєнням тієї чи іншої оцінки

з заданого діапазону (наприклад, висока ефективність, середня ефективність, низька ефективність), загальна оцінка буде грубо визначати ступінь захисту.

1.2 Огляд методів експертних оцінок

Метод експертних оцінок — це прадавній науковий метод, який дозволяє отримати об'єктивну оцінку на основі певної сукупності індивідуальних думок експертів. Слово «експерт» (expertus) у перекладі з латинської мови означає «досвідчений», що, в свою чергу, походить від слова «experire» — досліджувати. Експерт — це особа (спеціаліст), якому довірено висловити думку про якийсь суперечливий чи складний випадок, оскільки людство у складних ситуаціях завжди намагалося врахувати думку висококваліфікованих спеціалістів у різних сферах життєдіяльності.[11]

У випадках надзвичайної складності проблеми, її новизни, недостатності наявної інформації, неможливості математичної формалізації процесу вирішення доводиться звертатися до рекомендацій компетентних фахівців, які прекрасно знають проблему, – до експертів. Їх рішення задачі, аргументація, формування кількісних оцінок, обробка останніх формальними методами дістали назву методу експертних оцінок. [6]

Існує дві групи експертних оцінок:

1. Індивідуальні експертні методи полягають у використанні думок експертів відповідного профілю, сформульованих кожним із них, незалежно один від одного. оцінки засновані на використанні думки окремих експертів, незалежних один від одного. Основні переваги індивідуальних методів полягають у можливості використання здібностей і знань окремого експерта, а також у відносній простоті проведення цільового аналізу. Основний їхній недолік - обмеженість знань кожного з опитуваних про стан і розвиток суміжних сфер діяльності.

2. Колективні оцінки дозволяють задіяти групи експертів, добре обізнаних у багатьох суміжних сферах діяльності. Перевага колективних методів полягає в організації різними способами взаємодії між залученими фахівцями, що дає змогу проаналізувати проблему різнобічно.[9]

Способи вимірювання об'єктів

3. Ранжування – це розміщення об'єктів в порядку зростання або спадання будь-якої з їх властивостей. Ранжування дозволяє вибрати з досліджуваної сукупності факторів найсуттєвіший.

4. Парне порівняння – це встановлення переваги об'єктів при порівнянні всіх можливих пар. Тут не потрібно, як при ранжируванні, впорядковувати всі об'єкти, необхідно в кожній з пар виявити більш значимий об'єкт або встановити їх рівність.

5. Безпосередня оцінка. Часто буває необхідним не тільки впорядкувати (ранжувати об'єкти аналізу), але і визначити, на скільки один фактор найбільш значущий, ніж інші. В цьому випадку діапазон зміни характеристик об'єкта розбивається на окремі інтервали, кожному з яких приписується певна оцінка (бал). Саме тому метод безпосередньої оцінки іноді називають також бальним методом.

Метод простого ранжування полягає в тому, що кожного експерта просять розташувати ознаки в порядку переваги.

	1	2	…	j	…	m
1	a_{11}	a_{12}	…	a_{1j}	…	a_{1m}
2	a_{21}	a_{22}	…	a_{2j}	…	a_{2m}
…	…	…	…	…	…	…
i	a_{i1}	a_{i2}	…	a_{ij}	…	a_{im}
…	…	…	…	…	…	…
n	1_{ni}	a_{n2}	…	a_{nj}	…	a_{nm}

Рисунок 1.3 – Метод простого ранжування

a_{ij} - оцінка ознаки експертом, n - кількість ознак, m - кількість експертів.

Потім, підраховується S_i - середнє значення важливості ознаки.

Метод завдання вагових коефіцієнтів (a_{ij})

6. усім ознакам призначають вагові коефіцієнти так, щоб суми коефіцієнтів дорівнювали якомусь фіксованому числу (наприклад, одиниці, десяти або ста);

7. найбільш важливому з усіх ознак надають ваговий коефіцієнт, що дорівнює якомусь фіксованому числу, а всім іншим – коефіцієнти, рівні часткам цього числа.

Метод послідовних порівнянь полягає в наступному:

8. експерт впорядковує всі ознаки в порядку зменшення їх значимості: $A_1 > A_2 > ... > A_n$;

9. присвоює першій ознаці значення, рівне одиниці: A1 = 1, іншим же ознаками призначає вагові коефіцієнти в частках одиниці;

10. порівнює значення першої ознаки з сумою всіх наступних.

У парному порівнянні не потрібно, як при ранжируванні, впорядковувати всі об'єкти, необхідно в кожній з пар виявити більш значимий об'єкт або встановити їх рівність. Парне порівняння можна проводити при великому числі об'єктів, а також в тих випадках, коли відмінність між об'єктами настільки незначна, що практично нездійсненно їх ранжування.

При використанні методу частіше за все складається матриця розміром $n \times n$, де n - кількість порівнюваних об'єктів.

	1	2	...	j	...	n
1	a_{11}	a_{12}	...	a_{1j}	...	a_{1n}
2	a_{21}	a_{22}	...	a_{2j}	...	a_{2n}
...	...	...	...	...	...	...
i	a_{i1}	a_{i2}	...	a_{ij}	...	a_{in}
...	...	...	...	...	...	...
n	1_{ni}	a_{n2}	...	a_{nj}	...	a_{nn}

Рисунок 1.4 – Метод попарного порівняння

При порівнянні об'єктів матриця заповнюється елементами a_{ij} наступним чином (може бути запропонована і інша схема заповнення):

- 2, якщо об'єкт і краще об'єкта j (i> j),
- 1, якщо встановлено рівність об'єктів (i = j),
- 0, якщо об'єкт j краще об'єкта і (i <j).

1.2.1 Аналіз результатів експертних оцінок

Для подальшого аналізу результатів застосовуються різні методи математичної статистики. Вони можуть використовуватися окремо або комбінуватися в залежності від типу завдання і необхідного результату.

Формування узагальненої оцінки

Отже, нехай група експертів оцінила об'єкт, тоді x_j – оцінка j-го експерта, де m – число експертів.

Зазвичай узагальнена оцінка групи експертів формується с допомогою підрахування середніх величин, таких як медіана, середньо арифметична, квадратичне тощо.

Визначення відносних ваг об'єктів

Зазвичай необхідно освідомити істотність деякого фактору з точки зору будь-якого критерію. У цьому випадку говорять, що потрібно визначити вагу кожного фактора. Відрізняється від формування узагальненої оцінки тим, що визначається не загальна оцінка об'єкта, а оцінка для кожної його ознаки.

Встановлення ступеня узгодженості думок експертів

Коли ми працюємо з групою експертів ми затикаймося с ситуацією, коли розбіжність в їхніх оцінках неминучі, однак величина цієї розбіжності має важливе значення. Проте групова оцінка може вважатися достатньо надійною тільки за умови гарної узгодженості відповідей окремих фахівців.

Для аналізу розкиду і узгодженості оцінок застосовуються статистичні характеристики – заходи розкиду або статистична варіація.

Отже, способи обчислення заходів розкиду:

варіаційний розмах

$$R = x_{max} - x_{min}; \qquad (1.1)$$

середнє лінійне відхилення

$$a = \frac{1}{n}\sum_{i=1}^{n}|x_i - \bar{x}|, \tag{1.2}$$

середньоквадратичне відхилення

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}. \tag{1.3}$$

дисперсія

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2; \tag{1.4}$$

коефіцієнт рангової кореляції Спірмена

$$\rho = 1 - \frac{6\sum_{i=1}^{n}(x_{ij} - x_{ik})^2}{n(n^2-1)} = 1 - \frac{6\sum_{i=1}^{n} d_i^2}{n(n^2-1)}, \tag{1.5}$$

Коефіцієнт (величина ρ) змінюється в діапазоні від -1 до +1. При повному збігу оцінок коефіцієнт дорівнює одиниці. При найбільшому розбіжності в думках експертів спостерігається рівність коефіцієнта мінус одиниці.

x_{ij} - ранг (важливість), присвоєний і-му об'єкту j-им експертом, x_{ik} - ранг, присвоєний і-му об'єкту k-им експертом, d_i - різниця між рангами, присвоєними і-му об'єкту.

Коефіцієнт конкордації Кенделла

Коефіцієнт може приймати значення в межах від 0 до 1. При повній узгодженості думок експертів коефіцієнт конкордації дорівнює одиниці при повній незгоді – нулю. Найбільш реальним є випадок часткової узгодженості думок експертів.

Говорячи про узгодженість думок експертів, варто згадати, що ранжування не має на увазі (або не завжди має на увазі) відстань. Тобто у одного експерта A> B> C означає, що A >> B> C, а в іншого A> B >> C. І всякі кореляції і розрахунки середніх оцінок тут не допоможуть. Як варіант, вважати індекс узгодженості. Щось типо кількості суперечливих замкнутих ланцюжків думок експертів (Перший вважає, що А краще Б, другий, що Б краще С, а третій, що С краще А) до кількості всіх подібних ланцюжків.

Рейтинги зазвичай базуються на деякій ймовірнісній моделі, тому потрібно ретельно враховувати область їх можливого застосування.

1.3 Ефективність контролів інформаційної безпеки

Під терміном «контролю» у даній роботі розглядаються технічні та програмні засоби інформаційної системи, що виконують функції забезпечення стану захищеності інформаційної системі, протидіють реалізації вразливостей(атакам) або інформують про них.

Контролі інформаційної безпеки, що можуть бути використанів інформаційній системі можна поділити на дві групи: активні та пасивні. До активних контролів ІБ слід відносити такі, що мають можливість запобіганню реалізації атаки через загрози. До таких контролів можна віднести Firewall, DLP, антивірус тощо.

До пасивних контролів варто відносити такі засоби інформаційної безпеки, що виконують функції з обробки даних і стану системи та повідомляють про не типові події, та можливі атаки. До таких контролів можна віднести кореляційні правила SIEM-систем.

«Ефективність», як термін, залежно від галузі застосування може визначатися різним чином.

В загальному, наприклад за Оксфордським словником, ефективність (efficiency) — це знаходження в ефективному стані а також співвідношення корисної роботи машини до виділеного тепла. Визначення ближче до практики,

зокрема до інформаційних технологій можна отримати через термін «ефективний» - той, що досягає максимальної продуктивності з мінімальними витратами.

Проте значення ефективності можливо визначати за різними критеріями та розраховувати для широкого спектру параметрів.

Для вдалої оцінки ефективності контролів інформаційної безпеки варто використовувати статистичні дані про стан системи та події, що трапилися в ній та були класифіковані як інциденти ІБ, експертну оцінку стосовно ресурсів системи, суб'єктів, що виконують дії в системі та загроз, які присутні.

Ефективність, у даній роботі розглядається, як показник, що визначає, наскільки контроль зменшує ризик вдалої реалізації загрози.

Під поняттям «вдалої реалізації загрози» варто розуміти, такий сценарій подій при реалізації загрози, коли реалізація атаки через загрозу призвела до значних втрат ресурсів та коштів.

Висновок до розділу 1

У даному розділі були розглянуті основні етапи обробки інцидентів, зазначені методи підрахунку та обробки експертних оцінок та визначені основні поняття, що стосуються ефективності контролів ІБ.

Зроблено висновок, що необхідно розглянути існуючі методики оцінки ефективності та основні критерії на які вони спираються та проаналізувати за даними критеріями ефективність самих методів.

2 АНАЛІЗ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ КОНТРОЛІВ БЕЗПЕКИ

В даному розділі будуть описані та розглянуті існуючі методики оцінки ефективності та основні критерії на які вони спираються, проаналізовано за даними критеріями ефективність самих методів, та визначено ефективніші з них.

2.1 Опис методів

На сьогоднішній день Існують кількісні та якісні методи оцінювання ефективності. Виходячи с досвіду, можна побачити, що не дивлячись на свою узагальненість якісні методи не завжди є достатніми, коли постоє питання ефективності стану захищеності об'єктів, тобто кількісні методи теж повинні застосовуватися, для створення реальної ситуації. Для того, щоб визначити необхідні методи, потрібно мати чіткі та обгрунтовані показники оцінки ефективності системи(критерії). Зазвичай критерії можна поділити на наступні групи:

1. Критерії відношення корисного ефекту, до витрат. Тобто визначається ефективність залучених коштів по відношенню до отриманих результатів;
2. Критерії оцінювання якості контролів за визначеними показниками;
3. Штучно сконструйовані критерії, що дозволяють оцінювати інтегральний ефект (наприклад, «лінійна згортка» приватних показників, методи теорії нечітких множин).

При визначені ефективності та якості систем захисту можуть бути використані міжнародні стандарти ISO / IEC 17799 та ISO / IEC 15408. У першому з них пропонується розширений перелік аспектів інформаційної безпеки. Він починається з принципів розробки політики безпеки, включає основи перевірки системи на відповідність вимогам інформаційної безпеки, містить практичні рекомендації.

Стандарт ISO / IEC 15408 визначає критерії безпеки інформаційних технологій. У ньому не наводиться список вимог з безпеки, але положення стандарту дозволяють сформулювати цілі безпеки, спрямовані на забезпечення

протистояння загрозам і виконання політики безпеки, тобто ті цілі, які повинні використовуватися як основа для оцінки властивостей безпеки продуктів, систем та інформаційних технологій. Стандарт описує інфраструктуру, в якій користувачі системи можуть сформулювати вимоги, а експерти з безпеки визначити, чи володіє продукт заявленими властивостями.

Ефективність функціонування систем інформаційної безпеки та реалізованих у ній контролів безпеки залежить від багатьох взаємопов'язаних між собою елементів і, як правило, оцінюється сукупністю критеріїв, які перебувають в складних взаєминах. Відсутність на сьогоднішній день загального підходу до вирішення завдань даного класу тягне за собою різноманіття різних не взаємопов'язаних методів оцінювання ефективності.

Як вже було зазначено, процес визначення ефективності систем захисту починають з вибору і обґрунтування показників (критеріїв) оцінки ефективності системи захисту, а потім переходять до підбору або розробки методик розрахунку цих показників.

Далі наведемо основні методи, що використовуються на даний момент.

Статистичний. Статистичний метод оцінки базується на аналізі коливань досліджуваного показника за певний відрізок часу. Ступінь коливань показника має математично виражену імовірність настання небажаних наслідків, що базується на стохастичних даних і може бути розрахований достатньо точно.

Показник ефективності у даному випадку є те, що загроза і-го типу виникає в середньому за період часу Т.

Але слід зазначити, що закономірність змін аналізованої величини поширюється на майбутнє лише для тривалих періодів часу, а для короткотермінової оцінки екстраполяція минулих закономірностей дає значні помилки. У той же час слід враховувати, що при довгостроковому плануванні екстраполяція минулих середніх не враховує зміни обладнання, технологій та інші складові стратегічного планування. Тобто, проста екстраполяція не дає можливості реально оцінити стан системи. Отже, можна дійти висновку, що перевагою статистичного методу оцінки ризику є простота математичних розрахунків, а

суттєвим недоліком – необхідність великих обсягів вихідних даних (що більший масив, то достовірна оцінка).[13]

Ймовірнісний. Метод ґрунтується на аналізі випадкових, стохастичних подій, тобто таких подій, які в разі реалізації певної сукупності умов можуть відбутися або не відбутися. Він передбачає визначення як оцінки ймовірності виникнення загрози, так і розрахунок ймовірності того чи іншого шляху розвитку процесів, інакше кажучи – сценаріїв розвитку загрози. Ймовірності відповідного сценарію розвитку загрози оцінюють за допомогою методів теорії ймовірностей, математичної статистики, теорії випадкових процесів, теорії надійності, "дерева подій", "дерева відмов", а також методів суб'єктивної логіки (експертних оцінок).

Визначається ймовірність відмови системи від обробки даних в результаті реалізації загроз.

Сумарні середні втрати

$$R = \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} P\left(\frac{\vec{\gamma}}{\vec{s}}\right) P(\vec{s}) \Pi(\vec{\gamma}, \vec{s}) + m, \qquad (2.1)$$

$P\left(\frac{\vec{\gamma}}{\vec{s}}\right)$ - ймовірність усунення, $P(\vec{s})$ - апріорна ймовірність стану об'єкта контролю, $\Pi(\vec{\gamma}, \vec{s})$ - втрати прийняття рішення s при стані об'єкта. s, m - кількість розпізнаних загроз.[14]

Основні обмеження імовірнісного аналізу ризику пов'язані з недостатністю відомостей про функції розподілу параметрів випадкових величин, а також недостатньою статистикою щодо відмов устаткування і виникнення різних негативних подій.

Частотний. Метод є модифікацією статистичного методу, що спрямована не на загальну кількісну статистику загроз, а на частоту появи даних загроз, та підраховує збитки при вдалій реалізації загрози.

Очікуваний збиток від і-ї загрози:

$$R_i = F(S, V), \qquad (2.2)$$

де S — показник частоти виникнення загрози, V - умовний показник збитку.

На основі аналізу статистичного матеріалу задається значення S. Величина V вибирається рівною від 1 до максимально можливої суми збитку, розраховується значення показника R, як функції параметрів V і S.

Недоліки даного методу такі самі, як і у статистичного.

Експертне оцінювання. Як вже було зазначено, методи експертних оцінок – це спосіб прогнозування та оцінки результатів дій на основі прогнозів спеціалістів.

При реалізації методу експертних оцінок проводиться опитування групи експертів з метою визначення думки експертів стосовно певних відносних та змінних показників, що стосуються досліджуваного питання.

Важливою умовою правильного застосування методів експертної оцінки є висока обізнаність експерта з досліджуваної питання, здатність визначати чіткі вичерпні відповіді. Також, експерт не повинен бути зацікавленим в конкретному варіанті вирішення поставленої перед ним проблеми. Експерти підбираються за ознакою їх формального професійного статусу – посади, наукового ступеня, стажу роботи та ін. Такий підбір сприяє тому, що в число експертів потрапляють високопрофесійні, з великим практичним досвідом у даній галузі спеціалісти.[15]

У контексті інформаційної безпеки експертна оцінка може бути використана наступним чином:

Визначається кількість (n) і перелік параметрів (i) характеризують СЗІ. Задаються значення суб'єктивних коефіцієнтів важливості (W_i) кожної з характеристик G_i, призначені експертним шляхом. Розраховується значення параметра SR - ступінь забезпечення безпеки.

$$SR_{(s,r)} = \frac{1}{n}\sum_{i=1}^{n} W_i G_i \qquad (2.3)$$

Недоліком методу є значні витрати на компетентних експертів, втрата часу на ознайомлення з ситуацією та можлива не узгодженість експертів.

Матричний. Методика розроблена для використання в організаціях без залучення сторонніх фахівців і дає кількісні оцінки ризиків ІБ, проста у використанні і не вимагає використання програмного інструментарію.

Стан системи захисту описується трійкою параметрів, наприклад:

(S,O,M) – множини S - суб'єктів, O - об'єктів, M - прав доступу;

Або (O,H,M) - O - основи і складові частини системи (нормативно-правова, організаційна, інформаційна тощо), H - напрямки захисту, M - етапи створення СЗІ.

Основними кроками методу є:

1. Визначення параметрів.
2. Складання тривимірної матриці відносин.
3. Перетворення матриці відносин в двовимірну таблицю.
4. Визначення якісних і кількісних значень показників.

2.2 Порівняння методів

Для того щоб визначити найбільш зручні методики оцінки ІБ для організацій було проведено аналіз методик, розглянутих вище, за критеріями, які максимально задовольняють потребам організацій, а також відповідним їх можливостям.

Аналіз виконувався за сукупністю двох оцінок – максимальне значення оцінки за загальними характеристиками і мінімальне значення оцінки за вхідними даними.

Даний вибір обумовлений тим, що для організацій найбільш пріоритетними будуть критерії простоти використання методики, її ціна, і повнота результатів оцінки, а велика кількість вхідних даних для використання методики тільки ускладнить її застосування.

Результати порівняльного аналізу методик оцінки ризиків ІБ для організацій наведені в Таблиці 2.1.

Таблиця 2.1 - Порівняльний аналіз методик оцінки

Критерії порівняння	Найменування методики				
	Статистична	Ймовірніса	Частотна	Експертна	Матрична
загальні характеристики					
Методика рекомендована для організацій	0	1	0	1	1
Методика розрахована на організації різних областей діяльності	1	0	1	1	1
Простота використання	1	0	1	0	1
Розповсюджується безкоштовно	0	0	1	0	1
Кількісна оцінка	1	0	0	1	1
Якісна оцінка	0	1	1	1	1
Підвищення інформованості співробітників	0	0	0	1	1
Придатність до регулярного використання	0	1	0	1	1
Використання незалежної оцінки	0	0	0	1	0
РАЗОМ:	3	3	4	7	8
Вхідні дані					
Ресурси	1	1	1	0	0
Цінність ресурсів	1	1	1	1	1
Загрози	1	1	1	1	1
Уразливості	1	1	1	1	1
Вибір контрзаходів	0	1	0	1	1
Базові вимоги в області безпеки	0	0	1	1	0
Втрати	0	0	0	0	1
Заходи захисту інформації	0	1	1	1	1
Частота виникнення загроз	0	1	1	1	0
Мережеве обладнання	1	1	1	0	0
Види інформації	1	1	0	0	0
Групи користувачів	1	1	0	0	1
СЗІ	1	0	0	0	0
РАЗОМ:	8	10	8	7	7

Виходячи з результатів таблиці, можна зробити висновок, що найкращими відповідно до зазначених критеріїв, є Експертний та Матричний методи. Вони обидва дають змогу винести якісну та кількісну оцінки, придатні до регулярного

використання, підвищують інформованість співробітників та рекомендовані до застосування. Інші методи помітно відстають від них, через власну складність, значні кошти при реалізації та спроможності виносити лише якісну або кількісну оцінки.

Стосовно вхідних значень, всі методики досить схожі за потребами, проте Експертний та Матричний методи все одно потребують менше даних для свого чіткого функціонування.

Відповідно для створення більш ефективного методу варто використовувати саме ці методи для подальшого поєднання. Це дозволить перекрити слабкі сторони обох методів та використати сильні у повній мірі.

Висновок до розділу 2

В даному розділі було розглянуто існуючі методики оцінки ефективності та основні критерії на які вони спираються, проаналізовано за даними критеріями ефективність самих методів, та визначено ефективніші з них.

За результатами аналізу вийшло, що найефективнішими відповідно до зазначених критеріїв, є Експертний та Матричний методи.

Зроблено висновок, що для подальшого створення методу оцінювання ефективності, варто використовувати саме ці дві методики.

3 МЕТОД ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОНТРОЛІВ БЕЗПЕКИ

В даному розділі запропоновано метод оцінювання ефективності контролів інформаційної безпеки, що поєдную матричний та експертний підходи до оцінки ефективності.

3.1 Опис методу

У рамках даної магістерської роботи пропонується метод оцінювання ефективності контролів безпеки, що дозволяє розрахувати зменшення ризику вдалої реалізації загрози. Ефективність, у даній роботі розглядається, як показник, що визначає, наскільки контроль зменшує ризик вдалої реалізації загрози. Контролі безпеки, що розглядаються, можуть бути як активними, тобто які мають можливість впливати на ймовірність виникнення загрози, так і пасивними, тобто тими, що не можуть впливати на ймовірність виникнення загрози, але при гарному відпрацюванні процедури обробки інцидентів, вони можуть значно зменшити ризик вдалої реалізації загрози. Результати аналізу можуть бути використані при ухваленні рішення про модернізацію всього комплексу контролів інформаційної безпеки.

Пропонований метод заснований на використанні 3-х мірних матриць, куди заносяться матеріали обстеження і оцінювання та експертній оцінці. Весь процес включає наступні дії:

1. Визначити множини: суб'єктів, ресурсів, загроз.
2. Визначити ризик для зв'язки суб'єкт-ресурс-загроза.
3. Визначити застосований контроль.
4. Визначити коефіцієнт зниження ризику контролем по відношенню до загроз.
5. Розрахувати вплив контролю на ризики зв'язок суб'єкт-ресурс-загроза.
6. Розрахувати загальний ризик зв'язок суб'єкт-ресурс-загроза без контролю і з контролем.
7. Розрахувати зменшення ризику вдалої реалізації загрози.

3.2 Визначення множин суб’єктів, ресурсів та загроз

Перший етап полягає в інвентаризації елементів системи та аналізі можливих загроз. Виявляються елементи інформаційної системи, які підлягають захисту. У їх якості можуть виступати сукупності даних і технічні засоби, що забезпечують їх підтримку.

У розглянутій методиці потрібно чітко зазначити три множини та їх елементи, а самє:

- Суб’єкти - ролі, що існують в межах інформаційної системи, та можуть призвести до появи ризиків стосовно інформаційної безпеки;
- Ресурси - елементи інформаційної системи, що підлягають захисту, та втрата або пошкодження яких можуть призвести до фінансових втрат;
- Загрози - сукупність умов і факторів, що виникають у процесі взаємодії різних об'єктів (їх елементів) і здатних чинити негативний вплив на конкретний об'єкт інформаційної безпеки.

До множину Суб’єктів потрібно відносити функціональні ролі облікових записів, що існують в межах інформаційної системи. Не має потребі розглядати окрема кожний обліковий запис, тому потрібно згрупувати облікові записи по правам які вони мають у системі та діям які вони можуть виконати. Прикладом таких ролей можуть слугувати такі групи, як Адміністраторі та Користувачі.

До множини Ресурсів потрібно відносити ресурси, що є критично важливими у функціонуванні інформаційної системи та її бізнес-процесів. Тут вже слід враховувати специфіку кожного окремого компоненту, але для великих підприємств досить затратно проводити детальну інвентарізацію, тому для данного методу пропонується згрупувати ресурси. Прикладом таких груп можуть слугувати: Сервера, Робочі станції.

До множини Загроз слід відносити загрози, що створюють небезпеку порушення інформаційної безпеки. У розглянутій методиці для поняття

«інформаційна безпека» розглядається три аспекти: «Доступність», «Цілісність», «Конфіденційність». Шкідливий вплив на інформаційну систему може полягати в цілеспрямованому або випадковому впливі на будь-який аспект безпеки (можливо під впливом можуть виявитися два і навіть всі аспекти).

3.3 Визначення ризиків

Наступним кроком, після визначення множин потрібно створити 3-х мірну матрицю, розмірності $N \times S \times R$, кожен елемент якої буде відповідати ризику реалізації n-ї загрози, s-им суб'єктом на r-ому ресурсі.

Аналіз ризиків може бути виконаний з різним ступенем деталізації в залежності від критичності ресурсів, бізнес-процесів та попередніх інцидентів інформаційної безпеки. Методологія оцінки ризиків може бути кількісною або якісною, або їх комбінацією. На практиці якісна оцінка часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків. Кількісна оцінка ризиків є більш складною та потребує більше часу та ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Якісна методика оцінки ризиків використовує шкалу атрибутів для опису величини потенційних наслідків реалізації загроз. Перевагою якісної методики є її простота розуміння всім персоналом; недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз для кожного ресурсу системи.

Для виконання оцінки ризиків необхідно визначити шкалу для різних параметрів: оцінки величини наслідків реалізації загрози на аспекти інформаційної

безпеки, а саме «Доступність», «Цілісність», «Конфіденційність», оцінки ймовірності виникнення загрози.

Рекомендується використовувати такі шкали для оцінки ризиків:

Таблиця 3.1 - Для оцінки ймовірності виникнення загроз

Оцінка ймовірності	Опис
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Таблиця 3.2 - Для величини наслідків виникнення загрози: вплив на цілісність

Оцінка рівня наслідків	Опис
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат та має незначний вплив на репутацію підприємства
3	Призводить до значних фінансових втрат та має значний вплив на репутацію підприємства
4	Призводить до великих фінансових втрат, має значний вплив на репутацію підприємства і може призвести до зупинки роботи бізнес-процесу
5	Призводить до зупинки бізнес-процесу і порушує законодавство України

Таблиця 3.3 - Для величини наслідків виникнення загрози: вплив на конфіденційність

Оцінка рівня наслідків	Опис
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до “банківської таємниці”, “комерційної таємниці”, персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до “банківської таємниці”, “комерційної таємниці”, персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття документів, які відносяться до “банківської таємниці”, “комерційної таємниці”, персональних даних і призводить до значних фінансових втрат, має значний вплив на репутацію підприємства і може призвести до зупинки роботи бізнес-процесу
5	Призводить до зупинки бізнес-процесу і порушує законодавство України

Таблиця 3.4 - Для величини наслідків виникнення загрози: вплив на доступність

Оцінка рівня наслідків	Опис
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою для цього бізнес-процесу)
3	Вплив на доступність середній (не більше деякої частини від максимально допустимого часу простою для цього бізнес-процесу)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього бізнес-процесу)
5	Призводить до зупинки бізнес-процесу на тривалий час, який перевищує максимально допустимий час простою)

Визначення конкретних величин для параметрів оцінки повинно виконуватися з урахуванням досвіду, вимог нормативно-правових актів, історії попередніх інцидентів інформаційної безпеки, відомих випадків порушення інформаційної безпеки, досвіду інших установ тощо.

Наступним кроком, після визначення шкал, є зазначення впливу та ймовірності для кожного елементу матриці. Значення ризику, що буде вноситися до матриці буде рахуватися за класичною формулою перемноженням загального рівня оцінки величини наслідків на оцінку ймовірності виникнення загрози.

Загальний рівень оцінки величини наслідків розраховується за формулою довжини вектора у 3-х вимірному просторі, де проекцією на осі даного простору є значення аспектів інформаційної безпеки, а саме «Доступність», «Цілісність», «Конфіденційність».

Формула підрахунку ризику *n*-ї загрози, *s*-им суб'єктом на *r*-ому ресурсі:

$$L = \sqrt{a^2 + b^2 + c^2} \times p, \quad (3.1)$$

де L - ризик *n*-ї загрози, *s*-им суб'єктом на *r*-ому ресурсі, a - вплив на доступність, b - вплив на цілісність, c - вплив на конфіденційність, p - ймовірності виникнення загрози.

3.4 Визначення застосованих контролів та їх впливу на ризики

Наступним етапом після, визначення ризиків інформаційної системи, йде етап визначення застосованих контролів.

У даному етапі необхідно розглянути виділені контролі.

Для початкової оцінки контролів використовуємо метод експертної оцінки. Даний підхід був описаний у минулих розділах. Було зазначено, що існують дві групи експертних оцінок: індивідуальні та колективні. Рекомендовано використовувати колективні, через те що це позитивно відображається на правдивості оцінки, дозволяє зменшити ймовірність випадання з поля зору важливих показників та окремих вагомих випадків. Також важливим є вибір способу вимірювання, а саме визначення, який з трьох буде використовуватися групою експертів: ранжування, парне порівняння, безпосередня оцінка. Пропонується використовувати метод безпосередньої оцінки. Це зумовлено тим, що він дозволяє визначати значення в ситуаціях коли контролі як пов'язані, тобто впливають один на одного, так і не пов'язані.

Експертна група має обробити контроль, проаналізувати, в яких зонах інформаційної системи він буде працювати, які типи подій перехоплювати.

Розглянути статистично, які інциденти інформаційної безпеки вже були ним виявлені та наскільки вони були дійсними та достатніми, тобто визначити якість відпрацювання контролю в системі, на різних ресурсах та для різних типів користувачів.

Після ознайомлення з функціональними особливостями контролю, експертна група визначає наскільки успішно контроль може виявити загрозу та визначає коефіцієнт покриття контролем виявлення ознак загроз для кожної групи користувачів.

Рекомендується використовувати такі коефіцієнти:

Таблиця 3.5 - Коефіцієнт зниження ризику

Коефіцієнт	Опис
0	Контроль створено під дану загрозу
1	Контроль може виявити майже всі ознаки загрози
2	Контроль може виявити головні ознаки загрози
3	Контроль може виявити не головні ознаки загрози
4	Контроль може виявити ознаки у окремих випадках
5	Контроль не виявляє жодних ознак загрози

3.5 Розрахунок зменшення ризику вдалої реалізації загрози

На даному етапі проводиться розрахунок наступних показників:

- Впливу контролю на ризики зв'язок суб'єкт-ресурс-загроза.
- Загального ризик зв'язок суб'єкт-ресурс-загроза без контролю і з контролем.
- Зменшення ризику вдалої реалізації загрози.

Для розрахунку впливу контролю на ризики зв’язок, пропонується поділити 3-х мірну матрицю на множину з N 2-х мірних матриць, де N буде дорівнювати кількості визначених загроз, вплив контролю на які ми розглядаємо.

Вплив визначеного контролю на загрози в інформаційній системі буде визначатися за формулою:

$$\forall \triangle t_i (i \in [1;N]), c_{jt_i} (t_i \in \triangle c_j, j \in [1,M]): t_{ik} \times c_{jkt_i} = \triangle t'_j, \qquad (3.2)$$

де N- кількість матриць виділених по загрозам.

M- кількість розглянутих контролів.

t_i- загроза розглянута в i-й матриці для k-ого користувача.

c_{jkt_i}- коефіцієнт зниження ризику j-им контролем t_i-ої загрози для k-ого користувача.

t'_j - матриця ризиків після реалізації j-го контролю.

Після розрахунку впливу контролю на ризики при кожній окремій загрозі необхідно розрахувати загальний ризик після впровадження k-го контролю для f-ої загрози. Для проведення розрахунків використовуємо наступну формулу:

$$O_{kf} = \sqrt{\frac{\sum_{i=1}^{S} \sum_{j=1}^{R} (t'_{ij})^2}{Q}}, \qquad (3.3)$$

$$Q = S \times R ,$$

де O - загальний ризик після впровадження k-го контролю для f-ої загрози.

S - кількість суб’єктів.

R - кількість ресурсів.

t'_{ij}- значення ризику в комірках матриці після впровадження *k*-го контролю.

Q - загальна кількість елементів в матриці t'_j.

t'_j - матриця ризиків після реалізації j-го контролю.

Для оцінювання ефективності контролю, необхідно порівняти отримані результати після впровадження контролю з результатами при впровадженні контролю, що ніяк не вплинув на систему. Тобто, контроль, що не виявляє жодних ознак загрози, виду:

$$K = (5,5,\ldots,5)$$

Розрахунок ефективності контролю для *f*-ої загрози *k*-го контролю проводиться за допомогою формули, що показує зменшення ризику реалізації загрози після впровадження контролю:

$$\eta_{kf} = \frac{O_K - O_{kf}}{O_K} \times 100\%, \qquad (3.4)$$

де η_{kf}- ефективність *k*-го контролю для *f*-ої загрози.

O_K - загальний ризик контролю *K*, що не виявляє жодних ознак загрози.

Для розрахунку загальної ефективності контролю по всім розглянутим загрозам використовується формула середнього арифметичного:

$$\eta_{kA} = \frac{\sum_{f=1}^{N} \eta_{kf}}{N},$$

η_{kA}- ефективність *k*-го контролю.

N - визначена кількість загроз.

Після отримання загальної ефективності контролю, варто визначити,

чи є вона достатньою. Значення достатньої ефективності, тобто межі ефективності залежить від специфіки інформаційної системи, цілей, що намагаються досягти керівництво, та наявних ресурсів для реалізації контролів.

Висновок до розділу 3

В даному розділі було описано метод оцінювання ефективності контролів інформаційної безпеки у теоретичному вигляді. Описані послідовні етапи реалізації методу.

В результаті пропонується метод, що дозволяє розрахувати зменшення ризику вдалої реалізації загрози. Ефективність, у даній роботі розглядається, як показник, що визначає, наскільки контроль зменшує ризик вдалої реалізації загрози.

Зроблено висновок, що необхідно експериментально протестувати практичну реалізацію метода, для винесення рішення щодо його працездатності.

4 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОНТРОЛІВ БЕЗПЕКИ

В даному розділі буде розглянута методика проведення експерименту та описана практична реалізація методу оцінювання ефективності контролів інформаційної безпеки.

4.1 Методика проведення експерименту

Будь-яка розробка повинна підкріплюватися експериментальним дослідженням. Тобто виявлення якостей досліджуваних об’єктів, перевірка достовірності гіпотез, а також широке та глибоке вивчення досліджуваної наукової тематики. У рамках сучасної науки існує багато різних класифікацій експериментів в залежності від галузі науки, мети дослідження, структури об’єктів та явищ, організаційних заходів, характеру взаємодії об’єкту та засобів дослідження тощо.

Провідним місцем у досконалому проведенні експерименту, займає правильна розробка методики експерименту – визначена послідовність процесів, у результаті якої досягається мета дослідження.

Першочерговим етапом проведення експериментального дослідження є план програми дослідження, який складається за умови проведення дослідження, де визначається:

- гіпотеза;
- мета та задачі;
- вхідні і вихідні параметри, область їх визначення;
- порядок проведення власне експерименту;
- зазначаються необхідні засоби проведення дослідження, моделювання, обробки результатів;
- порядок і вимоги щодо оформлення результатів.

Далі, слідує етап визначення об’єму експериментальних досліджень та необхідних програмних та апаратних засобів тощо.

Останнім кроком є безпосередньо експеримент, який проводиться з регламентацією всіх кроків, та обробка і систематизація експериментальних і усіх числових даних, перевірка зведення до єдиної системи одиниць, побудова графіків залежностей, таблиць, діаграм тощо.

Гіпотеза

Експеримент базується на припущені, що запропонований метод оцінювання ефективності контролів безпеки адекватно реагує на зміну ідентифікуючих та оціночних параметрів при різних умовах контрольованого середовища.

Мета та задачі експерименту

Метою експерименту є перевірка адекватності запропонованого методу оцінювання ефективності контролів безпеки, а саме:

- дослідження запропонованого методу оцінювання ефективності контролів безпеки на основі експертних методів та матричного методу стосовно ефективності її роботи;
- тестування розробленого методу оцінювання ефективності контролів безпеки.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- обробка і верифікація отриманих результатів;
- визначення можливості використання методу оцінювання ефективності контролів безпеки.

Вибір вхідних та вихідних параметрів

Для методу оцінювання ефективності контролів безпеки

- вхідні параметри – обліковий запис індивідуальних користувачів, групи користувачів та ресурсів;
- вихідні параметри – показник ефективності контролів безпеки.

Послідовність дій в експериментальному досліджені

Дослідження методу оцінювання ефективності контролів безпеки виконуються в повній відповідності до етапів методу – проводиться тестування

розробленого методу оцінювання ефективності контролів безпеки, потім виноситься оцінка результатів тестування.

Засоби проведення експерименту

Для дослідження, створеного методу оцінювання ефективності контролів безпеки, імітаційного модулювання, обробки результатів та представлення їх в табличному та графічному вигляді використовувалося середовище Microsoft Excel 2007.

Аналіз результатів

Аналіз результатів імітаційного моделювання буде представлено у підрозділі 4.2 даної роботи. Результати представлені в табличній формі та у вигляді графіків і діаграм.

4.2 Тестування методу

Тестування запропонованого методу буде проводитися на основі кореляційних правил SIEM-системи ArcSight ESM, що є пасивними контролями безпеки, тобто тими, що не можуть впливати на ймовірність виникнення загори. Тестування пасивних контролів має свої власні особливості, які будуть розглянуті у експериментальній реалізації.

Першим етапом у запропонованому методі є визначення множин суб'єктів, ресурсів та загроз. Як вже було зазначено етап полягає в інвентаризації елементів системи та аналізі можливих загроз, що можуть реалізовуватися по відношенню до ресурсів.

Після проведення аналізу стану інформаційної системи, було виділено наступні групи елементи множини суб'єктів:

- Адміністратори - адміністративні облікові записи, що мають найширші повноваження і права в системі, на окремих або всіх її компонентах;

- Користувачі - облікові записи звичайних користувачів, що мають обмежені права, та виконують деяку діяльність лише на робочих станціях та на дозволених ресурсах системи;
- Зовнішні користувачі - облікові записи провайдерів зовнішніх послуг;
- Технічні облікові записи - записи для технічних дій в інформаційній системі.

До множини ресурсів відносимо:

- Сервери - серверна частина інфраструктури;
- Робочі станції - робочі станції працівників;
- Контролер домену - ресурс контролюючий область комп'ютерної мережі.

До множини загроз вплив на яких ми будемо розглядати відносимо:

- Bruteforce - перебір паролів;
- DoS - відмова в обслуговуванні;
- Аномальна активність користувача - нетипова або підозріла активність чи дії, виконані користувачем або його обліковим записом;
- Маскування дій користувача - приховування дій користувачів або спроба виконання дій від імені іншого користувача.

На основі зазначених елементів множин, що були оголошені на етапі підготовки, наступним кроком створюємо 3-х мірну матрицю, розмірності $N \times S \times R$, кожен елемент якої буде відповідати ризику реалізації n-ї загрози, s-им суб'єктом на r-ому ресурсі.

Відповідно до етапів запропонованого методу для підрахунку ризику, оцінюємо величини наслідків реалізації загрози на аспекти інформаційної безпеки, а саме «Доступність», «Цілісність», «Конфіденційність» та оцінюємо ймовірності виникнення загрози. Проте, через те, що контролі які ми тестуємо є пасивними, тобто тими, що не можуть впливати на ймовірність виникнення загори, то ми беремо за умову, те що загроза вже виникла. Тому значення ймовірності для даних контролів завжди буде дорівнювати одиниці, тобто $\rho = 1$. Вплив на аспекти задається відповідно до зазначених шкал.

У таблицях 4.1 - 4.3 наведено значення наслідків для аспектів інформаційної безпеки.

Таблиця 4.1 - Вплив на «Конфіденційність»

Загроза(Brutef orce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	3	4	5
Робочі станції	5	2	2	3
Контролер домену	5	0	4	5
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	3	0	2	2
Робочі станції	2	1	1	2
Контролер домену	3	0	2	3
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	3	3	5
Робочі станції	4	3	1	3
Контролер домену	5	1	2	4
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	1	1	5
Робочі станції	5	1	1	4
Контролер домену	5	0	2	3

Таблиця 4.2 - Вплив на «Цілісність»

Загроза(Brutef orce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	2	4	5
Робочі станції	5	3	3	3
Контролер домену	5	0	5	2
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	1	2	4
Робочі станції	4	4	1	3
Контролер домену	5	0	2	3
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	3	2	4
Робочі станції	3	3	2	2
Контролер домену	5	0	2	4
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	2	2	4
Робочі станції	5	4	3	1
Контролер домену	5	1	2	5

Таблиця 4.3 - Вплив на «Доступність»

Загроза(Brutef orce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	2	4	5
Робочі станції	5	3	3	3
Контролер домену	5	0	5	2
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	1	2	4
Робочі станції	4	4	1	3
Контролер домену	5	0	2	3
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	3	2	4
Робочі станції	3	3	2	2
Контролер домену	5	0	2	4
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	5	2	2	4
Робочі станції	5	4	3	1
Контролер домену	5	1	2	5

Як було зазначено, загальний рівень оцінки величини наслідків розраховується за формулою довжини вектора у 3-х вимірному просторі, де проекцією на осі даного простору є значення аспектів інформаційної безпеки, а саме «Доступність», «Цілісність», «Конфіденційність». А в зв'язку тим, що

контролі пасивні і їх ймовірність завжди дорівнює одиниці, після визначення загального рівня оцінки величини наслідків ми можемо отримати ризики для кожного елементу матриці.

У таблиці 4.4 підраховані ризики для елементів 3-х мірної матриці. Для зручності відображення вона зазначена у вигляді множини 2-х мірних матриць кожна з яких відповідає перерізу 3-х мірної матриці по деякій загрозі.

Таблиця 4.4 - Ризики зв'язок суб'єкт-ресурс-загроза

Загроза(Bruteforce)	Адміністратори	Користувачі	Зовнішній порушник	Технічні облікові запис
Сервери	8,660254038	3,605551275	7,549834435	8,660254038
Робочі станції	7,681145748	3,741657387	4,123105626	5,196152423
Контролер домену	8,660254038	0	7,549834435	7,348469228
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	7,681145748	4,123105626	5,744562647	6,708203932
Робочі станції	5,385164807	5,099019514	2,449489743	4,69041576
Контролер домену	7,681145748	1	4,898979486	5,830951895
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	4,242640687	5,385164807	7,071067812
Робочі станції	6,403124237	5,196152423	2,449489743	4,123105626
Контролер домену	8,660254038	1	4,123105626	6,403124237

Кінець таблиці 4.4

Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	2,236067977	3	7,071067812
Робочі станції	8,660254038	4,582575695	3,741657387	5,744562647
Контролер домену	8,660254038	1	3	6,557438524

Відповідно, мінімальне значення ризику для розглядуваного прикаду дорівнює нулю, тобто $L_{min} = 0$, а максимальне $L_{max} = 8{,}66$.

Наступним кроком методу, визначаємо застосовані контролі, та виносимо експертну оцінку зниження ризику відповідним контролем, через впроваджений коефіцієнт.

При створенні та впровадженні контролів інформаційної безпеки завжди необхідно розуміти специфіку підприємства. Але перелік основних контролів може бути досить універсальнім, адже структура сучасних підприємств досить подібна.

У даній роботі пропонується створювати контролі на основі стандарту ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements». Цей стандарт визначає вимоги щодо створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою в контексті організації. Він також включає вимоги до оцінки та обробки ризиків інформаційної безпеки, адаптованих до потреб організації. Вимоги, викладені в стандарті ISO / IEC 27001: 2013, є загальними і призначені для застосування до всіх організацій незалежно від типу, розміру та характеру.

Контролі будуть створюватися на основі доменів нормативу, а саме:

- Організація інформаційної безпеки(Organization of information security);
- Безпека людських ресурсів(Human resource security);

- Керування активами(Asset management);
- Керування доступом(Access control);
- Безпека операцій(Operations security);
- Безпека зв'язку(Communications security);
- Придбання, розробка та обслуговування системи(System acquisition, development and maintenance);
- Відносини з постачальниками(Supplier relationships).

Відповідно до зазначених категорій, створюються контролі інформаційної безпеки.

Проводити оцінювання ми будемо на основі наступних контролів:

- 09_01_Brute_force - контроль, що відпровідає домену Керування доступом(Access control), та створений для виявлення групи подій не успішної аутентифікації користувача в межах інтервалу часу;
- 09_02_Logon_anomaly - контроль, що відпровідає домену Керування доступом(Access control), та створений для виявлення аномалій при спробі аутентифікації користувачів;
- 07_01_Former_user_activity - контроль, що відпровідає домену Безпека людських ресурсів(Human resource security), та створений для виявлення появи системі активних подій з використанням облікових записів колишніх співробітників;
- 09_03_RunAs_detection - контроль, що відпровідає домену Керування доступом(Access control), та створений для виявлення подій використання одним обліковим записом інших та визначення подій маскування дій користувача.

Після ознайомлення з функціональними особливостями контролю, експертна група визначає наскільки успішно контроль може виявити загрозу та визначає коефіцієнт покриття контролем виявлення ознак загроз для кожної групи користувачів. Значення відповідних коефіцієнтів задаємо окремо по кожній групі з

множини суб'єктів, через те, що для різних типів облікових записів контроль може відпрацьовувати по різному. Також зазначимо варіант коли жоден контроль не буде впроваджений, тобто коефіцієнти будуть дорівнювати 5.

Значення відповідних коефіцієнтів визначено в таблиці 4.5.

Таблиця 4.5 - Коефіцієнт впливу контроля на зниження ризику

Система з відсутніми контролями	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Bruteforce	5	5	5	5
DOS	5	5	5	5
Аномальна активність користувача	5	5	5	5
Маскування дій користувача	5	5	5	5
09_01_Brute_force	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Bruteforce	0	1	2	1
DOS	4	2	5	3
Аномальна активність користувача	1	3	3	1
Маскування дій користувача	4	4	4	5
09_02_Logon_anomaly	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Bruteforce	1	2	2	1
DOS	2	2	2	3
Аномальна активність користувача	1	1	1	0
Маскування дій користувача	3	3	2	3

Кінець таблиці 4.5

07_01_Former_user_activity	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Bruteforce	4	3	2	5
DOS	4	3	5	5
Аномальна активність користувача	2	2	4	5
Маскування дій користувача	3	3	4	5
09_03_RunAs_detection	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Bruteforce	1	1	2	1
DOS	4	4	3	4
Аномальна активність користувача	2	1	1	1
Маскування дій користувача	1	1	0	1

Після визначення коефіцієнтів, відповідно до етапів методу, рахуємо наступні параметри:

- Вплив контролю на ризики зв'язок суб'єкт-ресурс-загроза.
- Загальний ризик зв'язок суб'єкт-ресурс-загроза без контролю і з контролем.
- Зменшення ризику вдалої реалізації загрози для кожного контролю.

Для розрахунку впливу контролю на ризики зв’язок, пропонується поділити 3-х мірну матрицю на множину з N 2-х мірних матриць, де N буде дорівнювати кількості визначених загроз, вплив контролю на які ми розглядаємо. Значення впливу контролів розраховується за формулою:

$$\forall \triangle t_i (i \in [1; N]), c_{jt_i} (t_i \in \triangle c_j, j \in [1, M]) : t_{ik} \times c_{jkt_i} = \triangle t'_j,$$

де N- кількість матриць виділених по загрозам.

M- кількість розглянутих контролів.

t_i- загроза розглянута в i-й матриці для k-ого користувача.

c_{jkt_i}- коефіцієнт зниження ризику j-им контролем t_i-ої загрози для k-ого користувача.

t'_j - матриця ризиків після реалізації j-го контролю.

У Таблицях 4.6 - 4.10 визначені впливи контролів.

Таблиця 4.6 - Значення ризиків без впливу контролів

Загроза(Bruteforce)				
	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	43,30127019	18,02775638	37,74917218	43,30127019
Робочі станції	38,40572874	18,70828693	20,61552813	25,98076211
Контролер домену	43,30127019	0	37,74917218	36,74234614
Загроза(DOS)				
	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	38,40572874	20,61552813	28,72281323	33,54101966
Робочі станції	26,92582404	25,49509757	12,24744871	23,4520788
Контролер домену	38,40572874	5	24,49489743	29,15475947

Кінець таблиці 4.6

Загроза(Аномальна активність користувача)				
	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	43,30127019	21,21320344	26,92582404	35,35533906
Робочі станції	32,01562119	25,98076211	12,24744871	20,61552813
Контролер домену	43,30127019	5	20,61552813	32,01562119
Загроза(Маскування дій користувача)				
	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	43,30127019	11,18033989	15	35,35533906
Робочі станції	43,30127019	22,91287847	18,70828693	28,72281323
Контролер домену	43,30127019	5	15	32,78719262

Таблиця 4.7 - Значення ризиків з урахуванням впливу контролю 09_01_Brute_force

Загроза(Brute force)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	0	3,605551275	15,09966887	8,660254038
Робочі станції	0	3,741657387	8,246211251	5,196152423
Контролер домену	0	0	15,09966887	7,348469228
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	30,72458299	8,246211251	28,72281323	20,1246118

Кінець таблиці 4.7

Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Робочі станції	21,54065923	10,19803903	12,24744871	14,07124728
Контролер домену	30,72458299	2	24,49489743	17,49285568
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	12,727922006	16,15549442	7,071067812
Робочі станції	6,403124237	15,588457227	7,348469228	4,123105626
Контролер домену	8,660254038	3	12,36931688	6,403124237
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	34,64101615	8,94427191	12	35,35533906
Робочі станції	34,64101615	18,330302778	14,96662955	28,72281323
Контролер домену	34,64101615	4	12	32,78719262

Таблиця 4.8 - Значення ризиків з урахуванням впливу контролю 09_02_Logon_anomaly

Загроза(Bruteforce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	7,211102551	15,09966887	8,660254038
Робочі станції	7,681145748	7,483314774	8,246211251	5,196152423

Кінець таблиці 4.8

Загроза(Bruteforce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Контролер домену	8,660254038	0	15,09966887	7,348469228
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	15,3622915	8,246211251	11,48912529	20,1246118
Робочі станції	10,77032961	10,19803903	4,898979486	14,07124728
Контролер домену	15,3622915	2	9,797958971	17,49285568
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	4,242640687	5,385164807	0
Робочі станції	6,403124237	5,196152423	2,449489743	0
Контролер домену	8,660254038	1	4,123105626	0
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	25,98076211	6,708203932	6	21,21320344
Робочі станції	25,98076211	13,74772708	7,483314774	17,23368794
Контролер домену	25,98076211	3	6	19,67231557

Таблиця 4.9 - Значення ризиків з урахуванням впливу контролю 07_01_Former_user_activity

Загроза(Bruteforce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	34,64101615	10,81665383	15,09966887	43,30127019
Робочі станції	30,72458299	11,22497216	8,246211251	25,98076211
Контролер домену	34,64101615	0	15,09966887	36,74234614
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	30,72458299	12,36931688	28,72281323	33,54101966
Робочі станції	21,54065923	15,29705854	12,24744871	23,4520788
Контролер домену	30,72458299	3	24,49489743	29,15475947
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	17,32050808	8,485281374	21,54065923	35,35533906
Робочі станції	12,80624847	10,39230485	9,797958971	20,61552813
Контролер домену	17,32050808	2	16,492422 5	32,01562119
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	25,98076211	6,708203932	12	35,35533906
Робочі станції	25,98076211	13,74772708	14,96662955	28,72281323
Контролер домену	25,98076211	3	12	32,78719262

Таблиця 4.10 - Значення ризиків з урахуванням впливу контролю 09_03_RunAs_detection

Загроза(Bruteforce)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	3,605551275	15,09966887	8,660254038
Робочі станції	7,681145748	3,741657387	8,246211251	5,196152423
Контролер домену	8,660254038	0	15,09966887	7,348469228
Загроза(DOS)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	30,72458299	16,4924225	17,23368794	26,83281573
Робочі станції	21,54065923	20,39607805	7,348469228	18,76166304
Контролер домену	30,72458299	4	14,69693846	23,32380758
Загроза(Аномальна активність користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	17,32050808	4,242640687	5,385164807	7,071067812
Робочі станції	12,80624847	5,196152423	2,449489743	4,123105626
Контролер домену	17,32050808	1	4,123105626	6,403124237
Загроза(Маскування дій користувача)	Адміністратори	Користувачі	Зовнішній провайдер	Технічні облікові запис
Сервери	8,660254038	2,236067977	0	7,071067812
Робочі станції	8,660254038	4,582575695	0	5,744562647
Контролер домену	8,660254038	1	0	6,557438524

Наступним кроком, після розрахунку впливу контролю на ризики при кожній окремій загрозі необхідно розрахувати загальний ризик після впровадження *k*-го контролю для *f*-ої загрози.

Для проведення розрахунків використовуємо формулу зазначену в методі. Дана формула дозволяє підрахувати загальний ризик, зменшуючи вплив максимальних та мінімальних показників, так як вони можуть псувати відображення реальної ситуації. Отримані дані відображені в Таблиці 4.11.

Таблиця 4.11 - Загальний ризик

	Система з відсутніми контролями	09_01_Brute_force	09_02_Logon_anomaly	07_01_Former_user_activity	09_03_RunAs_detection
Загроза(Bruteforce)	33,0088372	7,675719293	9,115005943	25,83763405	8,736894948
Загроза(DOS)	27,19528145	20,43689474	12,66557013	23,88863049	20,89457665
Загроза(Аномальна активність користувача)	28,75905654	9,92051746	4,907477288	19,32183566	8,990735973
Загроза(Маскування дій користувача)	29,22612986	25,32126906	17,15128761	22,2298598	5,61248608

Для оцінювання ефективності контролю, необхідно порівняти отримані результати після впровадження контролю з результатами при впровадженні контролю, що ніяк не вплинув на систему.

Розрахунок ефективності контролю для *f*-ої загрози *k*-го контролю проводиться за допомогою формули, що показує зменшення ризику реалізації загрози після впровадження контролю та задана в методі.

Для розрахунку загальної ефективності контролю по всім розглянутим загрозам використовується формула середнього арифметичного. Результати підрахунків винесені Таблиці 4.12.

Таблиця 4.12 - Ефективність контролів

	09_01_Brute_force	09_02_Logon_anomaly	07_01_Former_user_activity	09_03_RunAs_detection
Загроза(Brute force)	76,7%	72,4%	21,7%	73,5%
Загроза(DOS)	24,9%	53,4%	12,2%	23,2%
Загроза(Аномальна активність користувача)	65,5%	82,9%	32,8%	68,7%
Загроза(Маскування дій користувача)	13,4%	41,3%	23,9%	80,8%
Середні	45,1%	62,5%	22,7%	61,6%

Виходячи з даних Таблиці 4.12 ми можемо дати оцінку ефективності контролів та порівняти їх вплив на захищеність системи між один одним.

Значення достатньої ефективності задається в залежності від особливості підприємства та системи. У даному випадку слід вважати контроль ефективним, якщо він досягне значення в 50 відсотків. За результатами експерименту можна зробити висновок, що ефективними є два контролі - 09_02_Logon_anomaly та 09_03_RunAs_detection. Близьким до межі ефективності є контроль 09_01_Brute_force, а зовсім не ефективним є 07_01_Former_user_activity.

Висновок до розділу 4

В даному розділі була розглянута методика проведення експерименту та зроблена практична реалізація методу оцінювання ефективності контролів інформаційної безпеки. Описані послідовні етапи реалізації методу. підраховані проміжкові кроки та кінцевий результат.

В результаті визначено, що не всі запропоновані контролі задовольняють вимогам, та не досягають межі ефективності. Найбільше зменшує ризик вдалої реалізації загрози контролі 09_02_Logon_anomaly та 09_03_RunAs_detection.

Зроблено висновок, що запропонований метод є працездатним, та дозволяє оцінити ефективність контролів інформаційної безпеки.

5 СТАРТАП

5.1 Опис ідеї проекту (товару, послуги, технології)

Таблиця 5.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Дослідження ефективності активних та пасивних контролів безпеки	1. Захист інформації	Безпека інформаційних мереж
	2. Зменшення впливу атак. Інформаційна безпека	Захищеність інформаційних мереж
	3. Підвищення ефективності контролів безпеки	Стійкість інформаційних мереж

Конкурентами є аналогічні методи та механізми оцінювання ефективності контролів безпеки. Основною відмінністю є те, що метод оцінювання ефективності контролів безпеки реалізується таким чином, щоб забезпечити можливість порівняння ефективності контролів, для визначення найкращого для реалізації.

Довгостроковими перспективами є:

- Збільшення кількості клієнтів, що будуть використовувати запропоновані методи.
- Додавання новітніх механізмів захисту.

Потреби в стартовому фінансуванні:

Стартовий капітал = 5000 грн

Таблиця 5.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Конкурент1	Конкурент2	Конкур-рент3			
1.	Бюджетне фінансування	розробка за рахунок розробника	розробка за рахунок бюджетних коштів	розробка комерційна	розробка за рахунок розробника	відсутність фінансування	часткова бюджетне фінансування	бюджетне фінансування
2.	Використання сучасної техніки	використовується сучасна технік а	використовується застаріла технік а	використовується технік а застарілої конфігурації	використовується сучасна технік а	сучасна комплектація технікою	часткова комплектація технікою	технік а застарілої конфігурації
3.	Належна матеріально-технічна база	розробко проводиться за власні кошти на приватному ПК	бюджетна установа	інформаційний центр	інформаційний центр	інформаційний центр	бюджетна установа	власні кошти на приватному ПК
4.	Підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	є підключення до Інтернету	без підключення до Інтернету	часткова підключення до Інтернету	є підключення до Інтернету

Кінець таблиці 5.2

5.	Налагоджена система реклами продукту	продукт не рекламується	є реклама	продукт не рекламується	є реклама	не реклама	часткова реклама	рекламується
6.	Високий рівень розробки	запропоновані методи та алгоритми є досконалими	розробко не досконала та потребує доробок	запропоновані методи та алгоритми є досконалими	розробко не досконала та потребує доробок	розробко не досконала та потребує доробок	розробко є майже досконалою	запропоновані методи та алгоритми є досконалими
7.	Професіонали програмісти	розробка проводилася студентом	розробка проводилася групою професіоналів	розробка проводилася професіоналом програмістом	розробка проводилася професіоналом програмістом	розробка проводилася студентом	розробка проводилася професіоналом програмістом	розробка проводилася групою професіоналів
8.	Налагоджена співпраця із бізнес-структурами	ні	проводиться	ні	ні	ні	частково	проводиться

5.2 Технологічний аудит ідеї проекту

Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (табл. 5.3):

- за якою технологією буде виготовлено товар згідно ідеї проекту?

- чи існують такі технології, чи їх потрібно розробити/доробити?
- чи доступні такі технології авторам проекту?

Таблиця 5.3 –Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Дослідження ефективності активних та пасивних контролів безпеки	Технологія 1 (технологія надання послуги)	потрібно розробити	доступні
2		Технологія 2 (наявність бази досліджень)	наявні	доступні
3		Технологія 3 (база проведення досліджень (випробувань))	потрібно розробити	доступні
4		Технологія 4 (оформлення результатів дослідження)	потрібно розробити	доступні
Обрана технологія реалізації ідеї проекту: є можливою				

5.3 Аналіз ринкових можливостей запуску стартап проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів.

Таблиця 5.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	2
2	Загальний обсяг продаж, грн/ум.од	30000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	не має
5	Специфічні вимоги до стандартизації та сертифікації	ДСТУ В 7371:2013 ДСТУ ISO 9000-2007 (ISO 9000:2005, IDT) ДСТУ ITU-T G.957:2010
6	Середня норма рентабельності в галузі (або по ринку), %	30

На основі проведеного дослідження є можливість стверджувати про привабливість проекту для входження на ринок за попереднім оцінюванням.

Таблиця 5.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
	Підвищення ефективності контролів безпеки	Програмісти, інформаційні центрі, центри розвідки	формування рівня захищеності інформаційних мереж – програмісти; зниження рівня загроз – системні програмісти; визначення рівня атак – центри розвідки	відповідність ДСТУ В 7371:2013 ДСТУ ISO 9000-2007 (ISO 9000:2005, IDT) ДСТУ ITU-T G.957:2010 Обов’язкова наявність сертифікатів

Таблиця 5.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Агресивність конкурентів	вплив на систему	може порушити налагоджену систему розповсюдження
2	Нестабільність політичної ситуації в світі	балансування курсу	може порушити надійну систему постачальників
3	Висока вартість продукції	підвищення ціни	підвищить агресивність конкурентів
4	Економічні складності	відсутність фінансування	порушили фінансове забезпечення компанії

Таблиця 5.7 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
	Тривале існування	тривале існування на ринку	на ринку дає можливість виходу на нові ринки
	Моніторинг потреб споживачів	розуміючи потреби споживачів, розширювати діапазон продукції, що випускається.	розширення діапазону продукції, що випускається.
	Лібералізація торговельних бар'єрів	робота менеджменту	призведе до поліпшення налагодженої системи розповсюдження
	Висока вартість продукції в порівнянні з ключовими конкурентами	встановлення високої ціни	утруднить вихід на нові ринки
	Стабілізація бізнес-середовища	формування стабільного середовища	за рахунок стабілізації бізнес-середовища можна поліпшити фінансове забезпечення компанії

Таблиця 5.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Вказати тип конкуренції - монополія/олігополія/ монополістична/чиста	*Локальний/національний бізнес.*Глобальні сили є не досить вагомими по відношенню до локальних сил, які визначаються наявністю сертифікації, відповідності держ нормам і стандартам, регулюванням молокопереробної галузі державою.	працює в рамках оцінювання ефективності контролів безпеки
2. За рівнем конкурентної боротьби - локальний/національний/…	Локальний	Ведучи конкуренцію на локальному рівні, компанії необхідно прикласти належні зусилля для охоплення всього ринку
3. За галузевою ознакою - міжгалузева/ внутрішньогалузева	*Внутрішньогалузева.* Конкуренція на ринку ведеться в інформаційній галузі України	Необхідно зосередити зусилля на пошуку конкурентних переваг, які дозволять компанії займати стійкі конкурентні позиції
4. Конкуренція за видами товарів: - товарно-родова - товарно-видова - між бажаннями	*Товарно-родова.* Конкуренція на рівні технології задоволення потреб. Існує конкуренція з іншими моделями, алгоритмами	методи підвищення оцінювання ефективності контролів безпеки

Кінець таблиці 5.8

5. За характером конкурентних переваг - цінова / нецінова	*Нецінова.* При виборі алгоритмів та методів споживач звертає увагу на ефективність методів оцінювання ефективності контролів безпеки. *Цінова.* Для значної частки споживачів ціна є визначальною при виборі.	Головною конкурентною перевагою є унікальність позиціонування
6. За інтенсивністю - марочна/не марочна	*Марочна.*	Диференціація методів та моделей за мотивом задоволення потреб споживачів

Таблиця 5.9 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
	Навести перелік прямих конкурентів	Визначити бар'єри входження в ринок	Визначити фактори сили постачальників	Визначити фактори сили споживачів	Фактори загроз з боку замінників

Кінець таблиці 5.9

Висновки:	На ринку спостерігається тенденція до скорочення кількості підприємств і посилення конкуренції на ринку. Вступ України до СОТ відкрив дорогу іноземним виробникам. Великі компанії з іноземним капіталом постійно збільшують контрольовану ними частку ринку, поглинаючи конкурентів.	Бар'єри входу на ринок є порівняно незначними. Вартість організації бізнесу з виробництва сучасних механізмів підвищення оцінювання ефективності контролів безпеки сягає 100 тис. дол. Обов'язковою є сертифікація продукції.	Існує чітка залежність від постачальників як якості продукції. Також ціна кінцевої продукції залежить від рівня сертифікації.	Споживачі мають широку географію і проживають переважно у містах. Покупка програмних додатків та алгоритмів реалізації механізмів підвищення оцінювання ефективності контролів безпеки часто носить імпульсний характер.	Посилилася конкуренція зі сторони товарів субститутів – інших видів методів та алгоритмів підвищення оцінювання ефективності контролів безпеки, за рахунок збільшення асортименту останніх та появи нових для ринку категорій.

Отже, відповідно до наведеного вище аналізу головними силами, які діють на конкуренцію в галузі є постачальники та споживачі. Також в силу розвитку ринку все більшого значення набуває інтенсивність конкуренції між існуючими конкурентами та загроза зі сторони товарів-субститутуів.

Таким чином в межах структурного підходу до аналізу конкуренції тип конкуренції – *монополістична конкуренція*.

Таблиця 5.10 – Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	Обґрунтування вибору
1	Частка ринку	Враховуючи той факт, що тип родового середовища в галузі – консолідований ринок, тобто існує група компаній, які контролюють разом понад 40% ринку, а також те, що інтенсивність суперництва між діючими конкурентами при низьких темпах зростання ринку є однією з головних сил, які діють на конкуренцію в галузі, одним з найважливіших факторів конкурентоспроможності виступає частка ринку, яку займає виробник. В таких умовах чим більше частка ринку, тим більшими ринковими можливостями володіє виробник.
2	Ціна	Чим вигіднішою є ціна для споживача, тим вірогідніше його вибір.
3	Асортимент	В умовах збільшення інтенсивності між існуючими конкурентами завоювання споживачів відбувається за рахунок нових методів та алгоритмів.
4	Доступ до каналів розподілу	Споживач далеко не завжди проявляє прихильність до певної категорії розробників і дуже схильний до експериментів. В цьому випадку завоювати лояльність споживача дуже складно і ще складніше її утримати. Тому для компаній-виробників ключовими чинниками успіху стає сильна дистрибуція, якісний торговий маркетинг і налагоджена система логістики.
5	Торговий маркетинг	

Кінець таблиці 5.10

6	Рівень диференціації ТМ	В умовах ведення конкурентної боротьби на споживчому ринку, де попит є ірраціональним та існує велика кількість виробників і розробників при фактично відсутній різниці між товарами, що пропонуються, ключовим фактором успіху є здатність чітко диференціювати ТМ від ТМ конкурентів, надаючи споживачеві унікальну цінність.
7	Репутація виробника	Якщо компанія має бездоганну репутацію, особливо у сфері якості своєї продукції, то рівень довіри до неї зростає. Також репутація виробника важлива при виході на ринок з новими товарами, або при виході на нові сегменти, що полегшує позитивне сприйняття новинок.
8	Рівень лояльності до бренду	Чим вище рівень лояльності, тим більше компанія має прихильних, а значить постійних споживачів.
9	Унікальність позиціонування	В умовах монополістичної конкуренції, коли фактор диференціації ТМ є ключовим засобом ведення конкурентної боротьби, важливим є створення та підтримання унікального позиціонування, що створює певний захист від конкурентних зіткнень.
10	Маркетинговий бюджет	Від розміру маркетингового бюджету залежить здатність здійснювати маркетингову стратегію підприємства. Маркетингові заходи мають забезпечувати інші конкурентні переваги такі, як рівень диференціації, лояльності, репутація виробника, дистрибуція та просування в торгових точках.

Таблиця 5.11 – Порівняльний аналіз сильних та слабких сторін «Метод оцінювання ефективності контролів безпеки»

№	**Фактор конкурентоспроможності**	**Вагові значення фактора (1-20)**	**Рейтинг конкурентів у порівнянні з метод оцінювання ефективності контролів безпеки**						
			-3	**-2**	**-1**	**0**	**1**	**2**	**3**
1	Частка ринку	20		I		III	II		
2	Ціна	10					III	I	II

Кінець таблиці 5.11

3	Асортимент	18		III		I	II		
4	Доступ до каналів розподілу	15		II			III	I	
5	Торговий маркетинг	15					I	II	III
6	Рівень диференціації ТМ	13			I				
7	Репутація виробника	12	III	I,III					
8	Рівень лояльності до бренду	14			II	I	III		
9	Унікальність позиціонування	15	II	I	III				
10	Маркетинговий бюджет	10	II			III	I		

Умовні позначки позицій конкурентів:

I - конкурент 1

II - конкурент 2;

III - конкурент 3.

Отже, відповідно до проведеного аналізу можна сказати, що «Метод оцінювання ефективності контролів безпеки» має наступну позицію на ринку:

сильні сторони:

– унікальне позиціонування;
– значний рівень диференціації ТМ;
– позитивна репутація виробника;

слабкі сторони:

– вища ціна порівняно з конкурентами;
– торговий маркетинг.

Виділивши найвагоміші сильні та слабкі сторони «Метод оцінювання ефективності контролів безпеки» у порівнянні з основними конкурентами і з

аналізу внутрішніх факторів та використовуючи результати аналізу маркетингових загроз та можливостей, складемо матрицю SWOT-аналізу (табл. 5.12.).

Таблиця 5.12 – SWOT-аналіз стартап-проекту

Сильні сторони	**Слабкі сторони**
1. унікальне позиціонування; **2.** значний рівень диференціації **3.** позитивна репутація виробника; **4.** приналежність до української міжнародної компанії; **5.** налагоджена система дистрибуції товару; **6.** наявність вертикальної інтеграції.	**1.** вища ціна порівняно з конкурентами. **2.** залежність маркетингової політики від українського власника; **3.** слабке самозабезпечення фінансовими ресурсами; **4.** відсутність чітко вираженої маркетингової стратегії, непослідовність в її реалізації.
Можливості	**Загрози**
1. Можливість зміцнення іміджу **2.** Можливість збільшення обсягів реалізації **3.** Можливість збільшення обсягів продаж за рахунок експансії в регіони	**1.** Загроза працювати без прибутку скорочення платоспроможного попиту **2.** Загроза втрати споживачів внаслідок підвищення тиску зі сторони товарів-субститутів **3.** Загроза підвищення цін

З результатів SWOT-аналізу видно, що найбільш негативний вплив на діяльність «Метод оцінювання ефективності контролів безпеки» на ринку чинить ринкове середовище. Це, перш за все, пов’язано із наслідками фінансово-економічної кризи в країні.

В свою чергу, така ситуація супроводжувалася зменшенням темпів приросту галузі, виходом з ринку менш сильних дрібних та регіональних виробників,

приходом на ринок транснаціональних компаній, що збільшило інтенсивність конкуренції між діючими учасниками ринку України.

Було визначено, що найбільшою загрозою для «Метод оцінювання ефективності контролів безпеки» є загроза падіння прибутковості внаслідок скорочення попиту.

Таблиця 5.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1.	Використання засобів стимулювання збуту та мерчандайзингу в торгових точках для збільшення продаж	Дозволяє суттєво збільшити обсяги продаж	до місяця
2.	Розширення асортиментної лінійки	Можливість залучення нових споживачів за рахунок новинки	до пів року
3.	Збільшення представленості	Можливість розширення охоплення цільової аудиторії	до року

Найоптимальнішою є перша альтернатива

5.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл. 5.14).

Таблиця 5.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Метод оцінювання ефективності контролів безпеки	готовий	високий	мінімальна	простий
2	Зменшення впливу атак у безпроводових мережах	готовий	високий	максимальна	простий
3	Підвищення якості оцінювання ефективності контролів безпеки	готовий	високий	середня	простий

За результатами аналізу потенційних груп споживачів (сегментів) обрано стратегію диференційованого маркетингу.

Таблиця 5.15 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	Стратегія диференціації	передбачає надання товару важливих з точки зору споживача відмітних властивостей, які роблять товар відмінним від товарів конкурентів. Така відмінність може базуватися на об'єктивних або суб'єктивних, відчутних і невідчутних властивостях товару(у ширшому розумінні – комплексі маркетингу), бути реальною або уявною.	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).	Інструментом реалізації стратегії диференціації є ринкове позиціонування.

Таблиця 5.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
	Ні	к залучати нових так і забирати існуючих у конкурентів	частково	наслідування лідеру

Таблиця 5.17 – Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1	Відповідність чинним нормативам	Наслідування лідеру	Реалізація цієї стратегії вимагає, як правило, більш високих витрат. Проте успішна диференціація дозволяє компанії домогтись більшої рентабельності за рахунок того, що ринок готовий прийняти більш високу ціну (цінову премію бренду).	Унікальність Доступна ціна Реалізація нових методів

5.5 Розроблення маркетингової програми

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 5.18 підсумовуємо результати попереднього аналізу конкурентоспроможності товару.

Таблиця 5.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1.	Оцінка ефективності контролів безпеки	Безпека мереж	високий рівень безпеки мереж
2.	Зменшення впливу атак у безпроводових мереж	Захищеність мереж	високий рівень оцінювання ефективності контролів безпеки
3.	Підвищення оцінювання ефективності контролів безпеки	Стійкість безпроводових мереж	якість оцінювання ефективності контролів безпеки

Таблиця 5.19 – Опис трьох рівнів моделі товару

Рівні товару	*Сутність та складові*		
I. Товар за задумом	Опис базової потреби споживача, яку задовольняє товар (згідно концепції), її основної функціональної вигоди		
II. Товар у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	формування рівня оцінювання ефективності контролів безпеки – програмісти; зниження рівня загроз – системні програмісти; визначення рівня атак – центри розвідки		

Кінець таблиці 5.19

	Якість: ДСТУ В 7371:2013 ДСТУ ISO 9000-2007 (ISO 9000:2005, IDT) ДСТУ ITU-T G.957:2010
	Пакування – без пакування
	Марка: Метод оцінювання ефективності контролів безпеки
III. Товар із підкріпленням	До продажу – рівень розробки
	Після продажу – низка методів та алгоритмів
За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності	

Таблиця 5.20 – Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
	8000	7500	11000	2000-3000

Таблиця 5.21 – Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
	Мінімальна кількість посередників	організовувати широку мережу збуту товару	3	непряма

Таблиця 5.22 – Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Метод оцінювання ефективності контролів безпеки	інформаційні мережі	оцінювання ефективності контролів безпеки	донести переваги до потенційних користувачів	Основна ідея Оцінювання ефективності контролів безпеки
2	Захищеність мереж	інформаційні мережі	зменшення впливу атак у безпроводових мереж	донести переваги до потенційних користувачів	
3	Якість оцінювання ефективності контролів безпеки	інформаційна боротьба	підвищення оцінювання ефективності контролів безпеки	донести переваги до потенційних користувачів	

Висновок до розділу 5

В умовах розділу проведено аналіз та розробку бізнес-проекту до розробки «Метод оцінювання ефективності контролів безпеки», на основі проведеного аналізу варто відзначити, що найбільш негативний вплив на діяльність «Метод оцінювання ефективності контролів безпеки» на ринку чинить ринкове середовище. Це, перш за все, пов’язано із наслідками фінансово-економічної кризи в країні. В свою чергу, така ситуація супроводжувалася зменшенням темпів приросту галузі, виходом з ринку менш сильних дрібних та регіональних виробників, приходом на ринок транснаціональних компаній, що збільшило інтенсивність конкуренції між діючими учасниками ринку України. Було визначено, що найбільшою загрозою для «Метод оцінювання ефективності контролів безпеки» є загроза падіння прибутковості внаслідок скорочення попиту.

ВИСНОВКИ

В результаті дипломної роботи мета, яка полягала в дослідженні підходів до оцінювання ефективності контролів безпеки та реалізація методу оцінювання ефективності контролів безпеки може вважатися досягнутою.

Під час виконання роботи було визначено найпоширеніші механізми оцінювання ефективності. Розглянуті основні етапи обробки інцидентів, зазначені методи підрахунку та обробки експертних оцінок та визначені основні поняття, що стосуються ефективності контролів ІБ.

Проведено аналіз існуючих підходів до оцінки ефективності та основних критеріїв на які вони спираються, проаналізовано за даними критеріями ефективність самих методів, та визначено, що для подальшої реалізації методу варто використовувати два підходи - математичний та експертний. Це зумовлено тим, що вони отримали найкращі результати у порівнянні з іншими підходами та можуть бути об'єднані без виникнення конфліктів у логіці.

На основі проведеного аналізу підходів описано та реалізовано метод оцінювання ефективності контролів безпеки. Наведено та побудовано структуру системи оцінювання ефективності контролів безпеки, що спирається на запропонований метод та описує послідовність кроків реалізації методу для практичного застосування.

Розкрита методика проведення експерименту для визначення працездатності запропонованого методу. У ході експерименту досліджено практичну реалізацію методу оцінювання ефективності контролів безпеки та визначено, що не всі тестові контролі задовольняють заданим вимогам, та не досягають межі ефективності. Найбільше зменшує ризик вдалої реалізації загрози контролі 09_02_Logon_anomaly та 09_03_RunAs_detection.

За результатами експериментального дослідження зроблено висновок, що даний метод є працездатним, дозволяє якісно оцінити ефективність контролів інформаційної безпеки та провести порівняння тестових контролів відповідно до потреб підприємства

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ISO/IEC 27035-1:2016, Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management

2. ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements

3. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора [Текст] – 05540149.90000.044.И3-01-АЗ. – ІПСНАНУ, 2009. – С. 22-48.

4. Реагирование на инциденты информационной безопасности [Электронный ресурс]. – Режим доступа: https://it-community.in.ua/2014/07/reagirovanie-na-intsidenty-informatsionnoj-bezopasnosti.html/ - 05.08.2018

5. Tague, Nancy R. Plan–Do–Study–Act cycle. The quality toolbox (2nd ed.). – Milwaukee: ASQ Quality Press, 2005. – С. 390-392.

6. Громова Н.И. Основы экономического прогнозирования [Электронный ресурс]. – Режим доступа: https://www.monographies.ru/ru/book/section?id=166 – 15.09.2018

7. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання [Текст]. – Київ, ЛРІДУ, 2008. – С. 34-48.

8. Матвєев В. Експертні системи(конспект лекцій) [Электронный ресурс]. – Режим доступа: http://matveev.kiev.ua/exprt/t4.pdf – 15.09.2018

9. Новосад В. П., Селіверстов Р. Г. МЕТОДОЛОГІЯ ЕКСПЕРТНОГО ОЦІНЮВАННЯ [Текст]. – Вінниця, ВНТУ, 2010. – С. 10-31.

10. Вариация и вариационный ряд, Размах вариации [Электронный ресурс]. – Режим доступа: http://univer-nn.ru/statistika/variaciya-i-variacionnyj-ryad-razmax/ - 03.10.2018

11. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень [Текст]. – Маклаут, Київ, 2008. – С. 444.

12. Толюпа С.В., Підходи до проектування та оцінки ефективності системи захисту інформації в автоматизованих системах обробки та передачі даних [Текст]/ С.В. Толюпа, О.М. Іванова, І.О. Демченко // Науковотехнічний журнал “Сучасний захист інформації”. – 2013. – С. 25-30.

13. Страхарчук В.П. КОНЦЕПТУАЛЬНІ ЗАСАДИ КІЛЬКІСНОЇ ОЦІНКИ РИЗИКІВ [Текст]. – Суми: УАБС НБУ, 2004 – С. 278-287.

14. Маслова Н.О. Методи оцінки ефективності систем захисту інформаційних систем [Текст]. – Донецк: «Штучний інтелект» 4, 2008. – С. 253-264.

15. Методи експертних оцінок [Электронный ресурс]. – Режим доступа: https://pidruchniki.com/19650323/ekonomika/metodi_ekspertnih_otsinok - 03.10.2018